НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки
(повна назва інституту/факультету)

Кафедра звукотехніки та реєстрації інформації
(повна назва кафедри)

«На правах рукопису»
УДК 614.844: 681.327.8

«До захисту допущено»
Завідувач кафедри
_____ _____
(підпис) (ініціали, прізвище)
“___”_____20__ р.

Магістерська дисертація

зі спеціальності (спеціалізації) 171 Електроніка (Електронні системи мультимедіа та засоби Інтернету речей)
(код і назва спеціальності)

на тему: «Дослідження технічних особливостей впровадження інтегрованої комплексної системи безпеки спеціального об'єкту».

Виконав студент __VI__ курсу, групи __ДВ-82мп__
(шифр групи)

Безпрозванний Микола Олександрович
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник доц., к.т.н. Трапезон К.О.
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2019 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»

Інститут (факультет)_____Факультет електроніки_____
(повна назва)

Кафедра _____Кафедра звукотехніки та реєстрації інформації_____
(повна назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (спеціалізація) 171 Електроніка (Електронні системи мультимедіа та засоби Інтернету речей)_____
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ _____
(підпис) (ініціали, прізвище)

«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту
_____Безпрозванного Миколи Олександровича_____
(прізвище, ім'я, по батькові)

1. Тема дисертації Дослідження технічних особливостей впровадження інтегрованої комплексної системи безпеки спеціального об'єкту.
науковий керівник дисертації____доц., к.т.н., Трапезон К.О._____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «07» листопада 2019р. №3859-с

2. Строк подання студентом дисертації 09.12.2019р._____

3. Об'єкт дослідження Об'єктом дослідження є технічні особливості впровадження інтегрованої комплексної системи безпеки спеціального об'єкту

4. Предмет дослідження (Вихідні дані – для магістерської дисертації за освітньо-професійною програмою) 1) технології побудови інтегрованих комплексних систем безпеки спеціальних об'єктів. 2) охоронні, пожежні системи безпеки; системи відеонагляду; параметр який аналізується – рівень захищеності об'єкту; спеціалізоване програмне забезпечення для розробки та демонстрації моделей систем безпеки та відеонагляду.

5. Перелік завдань, які потрібно розробити: Провести розгляд основних елементів базової домашньої охоронної системи та визначити можливість їх використання при створенні комплексної охоронної системи для спеціального об’єкту. Дослідження напрямків забезпечення захищеності об’єкту, визначення на їх основі основних частин для проектування комплексної інтегрованої системи. Розгляд інженерних та програмних рішень по створенню інтегрованої комплексної системи охорони об’єкту на основі технічних засобів “Болід”.

6. Перелік графічного (ілюстративного) матеріалу 47 рисунків у роботі, 18 таблиць, 1 презентація, 10 слайдів.

7. Орієнтовний перелік публікацій «».

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання 20.10.2018

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
	Написання першого розділу: «Особливості створення домашніх охоронних систем».	11.10.2019	
	Написання другого розділу: «Аналіз методів створення інтегрованих комплексних систем безпеки спеціальних об'єктів».	23.10.2019	
	Написання третього розділу: «Розробка моделі інтегрованої комплексної системи безпеки спеціального об’єкту».	04.11.2019	
	Написання четвертого розділу: «Розроблення стартап-проекту».	12.11.2019	
	Підготовка матеріалів до друку та оформлення пояснювальної записки	26.11.2019	
	Підготовка та оформлення презентації для доповіді	30.11.2019	

Студент _____ М.О. Безпрозванний
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ К. О. Трапезон
(підпис) (ініціали, прізвище)

УДК 614.844: 681.327.8

РЕФЕРАТ

Магістерська дисертація: 102 с., 47 рис., 18 табл., 12 джерел.

СЕНСОР, ОХОРОННО-ПОЖЕЖНА СИСТЕМА, СИСТЕМА ВІДЕОНАГЛЯДУ, ІНТЕГРОВАНА КОМПЛЕКСНА СИСТЕМА.

Актуальність роботи полягає у тому, що на сьогоднішній день забезпечення власної безпеки, а також охорони рухомої та нерухомої власності стало не примхою, а необхідністю. Рішення даної задачі можливе тільки при грамотному оснащенні систем безпеки сучасними високонадійними технічними засобами охорони. Тому попит на новітні та високонадійні системи зараз тільки безпеки зростає.

Об’єктом дослідження є технічні особливості впровадження інтегрованої комплексної системи безпеки спеціального об'єкту

Метою дослідження є визначення особливостей проектування в спеціалізованому програмному забезпеченні комплексної охоронної системи спеціального об’єкту з наданням можливості її удосконалення до новітніх технологій Інтернету речей. Так, передбачається, створити високозахищену модель спеціального об'єкту з сучасними високонадійними технічними засобами охоронних систем.

Для досягнення мети були поставлені такі завдання:

1. Провести розгляд основних елементів базової домашньої охоронної системи та визначити можливість їх використання при створенні комплексної охоронної системи для спеціального об’єкту.

2. Дослідження напрямків забезпечення захищеності об’єкту, визначення на їх основі основних частин для проектування комплексної інтегрованої системи.

3. Розгляд інженерних та програмних рішень по створенню інтегрованої комплексної системи охорони об’єкту на основі технічних засобів “Болід”.

SUMMARY

Master's dissertation: 104 p., 47 pic., 18 tables, 12 sources.

SENSOR, SECURITY & FIRE SYSTEM, CCTV SYSTEM, INTEGRATED COMPLEX SYSTEM.

The urgency of the work lies in the fact that to date, ensuring their own safety, as well as protection of movable and immovable property has become not a whim but a necessity. The solution to this problem is possible only with the competent equipping of security systems with modern highly reliable technical means of protection. Therefore, the demand for the latest and most reliable systems is now only increasing.

The object of the study is the technical features of the integrated integrated security system of the special object

The purpose of the study is to determine the design features in specialized software integrated security system of a special object with the opportunity to improve it to the latest technologies of the Internet of Things. So, it is supposed to create a highly protected model of a special object with modern highly reliable technical means of security systems.

To achieve this goal, the following tasks were set:

1. Review the basic elements of a basic home security system and determine whether they can be used when creating a complex security system for a special object.

2. Investigating the areas of object security, identifying the essential parts for designing a comprehensive integrated system based on them.

3. Consideration of engineering and software solutions for the creation of an integrated complex system of object protection based on Bolid technical equipment.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІЧ-сенсор	–	Сенсор з чутливим елементом, що реагує на інфрачервоне випромінювання;
НВО	–	науково виробничого об’єднання;
AAC	–	Advanced Audio Coding;
AVI	–	Audio Video Interleave;
BNC	–	Bayonet Neill-Concelman;
DVR	–	Digital Video Recorder;
G.711	–	Рекомендація ITU-T – міжнародний стандарт для модуляції мовних сигналів;
G.726	–	Кодек є стандартом ITU-T адаптивної імпульсно-кодової модуляції;
GSM	–	Global System for Mobile Communications
HDMI	–	High Definition Multimedia Interface
H.264	–	Advanced Video Coding;
MJPEG	–	Motion JPEG – покадровый метод видеосжатия;
MPEG-4	–	Moving Picture Experts Group;
PCM	–	Pulse Code Modulation;
Pelco-D	–	Протокол управління камерою, що використовується в галузі відеоспостереження;
Pelco-P	–	Протокол управління камерою, що використовується в галузі відеоспостереження;
PTZ-камера	–	Pan / Tilt / Zoom камера;
RS-485	–	Recommended Standard 485;
RS-232	–	Recommended Standard 232;
TCP/IP	–	Transmission Control Protocol/Internet Protocol
VGA	–	Video Graphics Array;
Wi-Fi	–	Wireless Fidelity.

ВСТУП

У наш час забезпечення власної безпеки, а також охорони рухомої та нерухомої власності стало не примхою, а необхідністю. Рішення даної задачі можливе тільки при грамотному оснащенні систем безпеки сучасними високонадійними технічними засобами охорони. Клієнтами охоронних компаній стають все більше людей, це і власники квартир, приватних маєтків, підприємств, організацій, транспортних засобів та навіть стратегічні об’єкти у держаній власності.

Попит на новітні та високонадійні системи безпеки зростає, тому компанії виробники таких систем постійно знаходяться у атмосфері жорсткої конкуренції, яка спонукає їх до стрімкого технічного розвитку. Саме тому розробку вдосконаленої моделі інтегрованої комплексної системи безпеки спеціального об'єкту вважаю **актуальною темою магістерської дисертації.**

Метою дослідження є визначення особливостей проектування в спеціалізованому програмному забезпеченні комплексної охоронної системи спеціального об’єкту з наданням можливості її удосконалення до новітніх технологій Інтернету речей. Так, передбачається, створити високозахищену модель спеціального об'єкту з сучасними високонадійними технічними засобами охоронних систем.

Для досягнення мети були поставлені такі завдання:

1. Провести розгляд основних елементів базової домашньої охоронної системи та визначити можливість їх використання при створенні комплексної охоронної системи для спеціального об’єкту.

2. Дослідження напрямків забезпечення захищеності об’єкту, визначення на їх основі основних частин для проектування комплексної інтегрованої системи.

3. Розгляд інженерних та програмних рішень по створенню інтегрованої комплексної системи охорони об’єкту на основі технічних засобів “Болід”.

Об’єктом дослідження є інтегрована комплексна система безпеки спеціального об’єкту.

Новизна роботи полягає в розробці вдосконаленої моделі інтегровананої комплексної системи безпеки спеціального об’єкту.

Практична цінність полягає у визначення передумов, які слід враховувати при реалізації технічних рішень на різних етапах створення системи охорони об’єкта.

1 ОСОБЛИВОСТІ СТВОРЕННЯ ДОМАШНІХ ОХОРОННИХ СИСТЕМ

1.1 Визначення та класифікація домашніх охоронних систем

Система безпеки – автоматизований комплекс для охорони різних об'єктів майна (будівель, включаючи прилеглу до них територію, окремих приміщень, автомобілів, водного транспорту, сейфів та ін.). Головне призначення охоронної системи це в першу чергу унеможливлення несанкціонованого проникнення в приміщення, що знаходиться під охороною та оперативне і гарантоване сповіщення господарів і правоохоронних служб про спробу здійснення незаконних дій щодо майна в приміщенні або самого об'єкту що охороняється. А також можливість розпізнати злочинців з записів відеоспостереження або навіть затримати на місці злочину за допомогою активних систем безпеки.

Система безпеки це узагальнюючий термін для декількох типів систем, а саме: контролю доступу, охоронної та пожежної сигналізації, відеонагляду, систем охорони активної дії.

Класифікація домашніх систем безпеки приміщень.

За взаємодією із загрозою:

– Пасивні – під час спрацювання таких систем власник або служби охорони отримують сповіщення про проникнення в приміщення;

– Автономна охоронна система – засоби, що діють локально привертаючи увагу звуком та світловими ефектами.

– Централізована пультова сигналізація – при спрацьовуванні такої сигналізації на об’єкті, за викликом про проникнення в приміщення, що охороняється вирушає оперативна группа охорони.

За способом передачі інформації:

– Проводові – лінії витої пари, оптиковолоконні та телефонні;

– Безпроводові — в них охоронні сенсори надсилають інформацію на приймальний засіб за допомогою радіохвиль.

1.2 Аналіз розміщення елементів домашніх систем безпеки

Базова система передбачає установку охоронних сенсорів, здатних перекрити всі потенційні зони проникнення. Датчики встановлені таким чином, щоб зловмисник не міг проникнути в приміщення, залишаючись при цьому непоміченим. Розміщення подібне до рис. 1.1 зумовлене зоною виявлення в 12 м (в різних моделях може бути більшою або меншою).

Як і для автономної так і для «пультової» охорони топологія рис. 1.2 може бути однаковою оскільки системи охорони з використання безпроводової технології вже достатньо давно співпрацюють з охоронними службами. Це може бути постановка на пульт через інтерфейс хабу чи централі, або окремого безпроводового пульту управління.

Рисунок 1.1 – Вид згори на розміщення пристроїв домашньої охоронної системи в приміщенні

Рисунок 1.2 – Типова топологія мереж домашньої охоронної системи

Але не лише сповіщувачі можуть ефективно боротися проти потенційних проникнень. Системи відеоспостереження вчасно і з високою точністю сповістять про проникнення на об’єкт що знаходиться під охороною та запишуть усі необхідні дані для розслідування правоохоронними органами цього випадку.

Відеоспостереження вже давно є невід'ємною частиною нашого життя.

Воно активно використовується для забезпечення безпеки комерційних об'єктів, громадських місць і приватних домоволодінь.

З розвитком Інтернету речей та інформаційних технологій інтелектуальність систем відеоспостереження істотно зросла, і вони зараз стають розумним в буквальному сенсі цього слова.

Система розумного відеоспостереження являє собою сукупність відеокамер і сенсорів, об'єднаних на базі технології Інтернету речей (IoT).

Один з варіантів побудови системи представлений зображено на рис. 1.2 нижче.

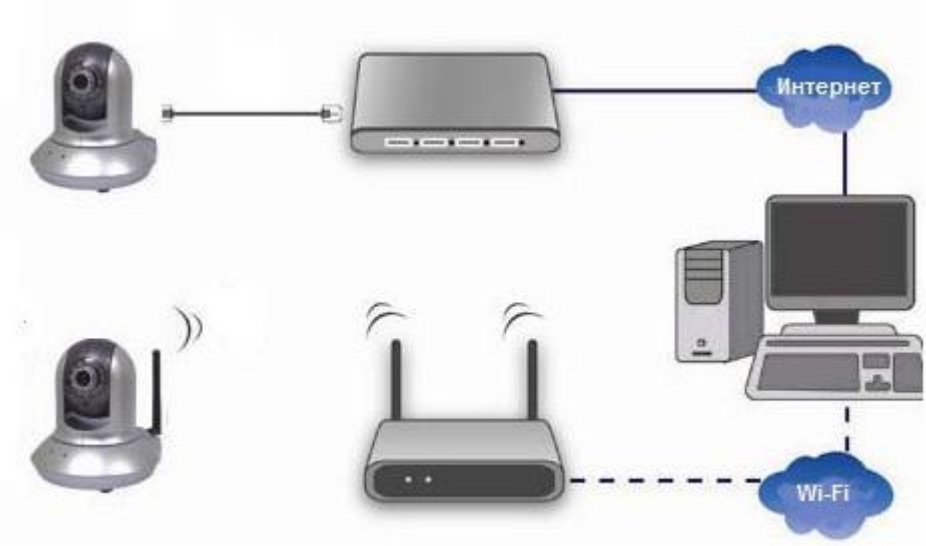


Рисунок 1.3 – Типова архітектура системи домашнього відеоспостереження

Структура домашньої охоронної системи:

– устаткування централізованого управління охоронною системою-централь зі встановленим на ньому ПЗ для управління та контролю за сигналізацією;

– пристрої збору і обробки інформації з давачів охоронної сигналізації: прилади приймально-контрольні охоронні (панелі);

– сенсорні пристрої – датчики охоронної сигналізації.

1.3 Висновки

Розглянутих засобів безпеки може виявитися недостатньо, особливо для охорони спеціальних об’єктів. І забезпечення надійного захисту спеціального об’єкту неможливо без використання інтегрованих комплексних систем безпеки, що включають в себе багаторівневу систему контролю та управління доступом, високотехнологічні та надчутливі охоронно-пожежні сенсори, сичтеми відеонагляду з можливістю

розпізнавання об’єктів, спеціалізовані системи оповіщення і т.д. Можна виділити наступні переваги впровадження подібних систем безпеки [5]:

– підвищений рівень безпеки об’єкта в цілому та запобігання аварій – забезпечення безперервності процесів контролю та управління;

– організація мережевої структури управління з реалізацією функцій автоматичного контролю, обробки, аналізу та зберігання інформації про стан систем і дій оператора системи з єдиного диспетчерського пульта управління;

– можливість інтеграції на інформаційному рівні (протокол обміну) з системами різних підрозділів підприємства.

2 АНАЛІЗ МЕТОДІВ СТВОРЕННЯ ІНТЕГРОВАНИХ КОМПЛЕКСНИХ СИСТЕМ БЕЗПЕКИ СПЕЦІАЛЬНИХ ОБ'ЄКТІВ

2.1 Основи формування комплексу технічних засобів забезпечення безпеки

Реалізація концепції безпеки передбачає кілька напрямків забезпечення захищеності об'єкта – це економічна, науково- технічна, технологічна, екологічна, інформаційна, інженерно-технічна безпека. Всі вони є елементами єдиної системи комплексної безпеки даного об'єкту.

До складу комплексу технічних засобів забезпечення безпеки спеціального об'єкту повинні входити наступні технічні підсистеми [5, 9, 12]:

- охоронної та тривожної сигналізації;
- пожежної сигналізації;
- контролю і управління доступом;
- відеоспостереження;
- огляду і пошуку;
- пожежної автоматики (пожежогасіння, протидимного захисту);
- оповіщення та управління евакуацією;
- засоби оперативного зв'язку з об'єктом;
- захисту інформації;
- інженерно-технічної укріпленості;
- інженерного забезпечення об'єкта.

Склад і кількість об'єктових підсистем безпеки можуть варіюватися залежно від призначення об'єкта, що захищається і конкретних умов з комплексного забезпечення його безпеки.

2.2 Структура комплексної системи безпеки

Будемо розглядати задачу забезпечення захисту об'єкта силами чотирьох основних нероздільних підсистем комплексу технічних засобів забезпечення безпеки, окремо виконують свої функції: системи охоронної і тривожної сигналізації, системи пожежної сигналізації, системи контролю та управління доступом, системи охоронної телевізійної. Комплекс доповнюють різні допоміжні пристрої, наприклад, системи електроживлення, охоронного освітлення, оповіщення, запобігання і ліквідації загроз і інші системи, які забезпечують життєздатність і надійне функціонування основних підсистем.

Кожна з основних підсистем може розглядатися як комплексна системи безпеки, яка відпрацьовує свій комплекс загроз і включає в себе сукупність технічних засобів охорони. Технічні засоби охорони (ТЗО) є базовим поняттям, що позначає апаратуру, яка використовується в складі комплексів забезпечення безпеки об'єктів від несанкціонованого проникнення.

Структура комплексної системи безпеки виконується за класичною схемою і складається з наступних елементів [1, 9, 12]:

– СЗОІУЦ (система збору та обробки інформації та управління центральна) – сервер, де зберігаються і обробляються всі бази даних системи; контрольні панелі, пульти, консолі управління; в загальному випадку входить до складу центрального пульта спостереження поряд з автоматизованими робочими місцями (АРМ) операторів, адміністраторів систем, постів охорони та служби безпеки;

– СЗОІУП (система збору та обробки інформації та управління периферійна) – пристрої (контролери, розширювачі, пульти управління), безпосередньо на апаратному рівні взаємодіючі зі своїми сенсорами, сенсорами або виконавчими пристроями, а на інформаційному рівні зв'язують їх ПЗ локальному інтерфейсу (RS-485, RS-232) з робочими станціями або з сервером;

– ЗВЗ (засоби виявлення загроз) – сенсори охоронної, тривожної, пожежної сигналізації, зчитувачі, клавіатури, відеокамери;

– СПП (система передачі повідомлень) – канали і засоби передачі службових та тривожних сповіщень, візуальної та акустичної інформації про об'єкт і стан системи безпеки;

– ЛКМ (локальна комп'ютерна мережа) – інформаційно зв'язує в єдиний комплекс окремі компоненти системи;

– ПЗ – мережеве, системне і прикладне програмне забезпечення сервера і робочих станцій, а також вбудоване програмне забезпечення системних контролерів, контрольних панелей і модулів;

– СБЖ (система гарантованого безперебійного електроживлення), яка включає в себе:

– електрощитову, підключену до мережі 220В, що містить всі необхідні вхідні і вихідні силові автомати;

– джерела безперебійного живлення (ДБЖ), що забезпечують безперервне і якісне електроживлення всієї апаратури;

– розведену ПЗ всьому об'єкту окрему мережу живлення з розміщенням при необхідності окремих ДБЖ в спеціально виділених приміщеннях, нішах або шафах, які перебувають під охороною.

– ДП – допоміжні пристрої, які забезпечують виконання системою охорони ряду функцій і включають в себе:

– ЗО – засоби оповіщення;

– ЗВІ – засоби відображення інформації;

– ЗРД – засоби реєстрації даних;

– ЗПЛЗ – засоби протидії та ліквідації загроз.

Узагальнена структурна схема комплексної системи безпеки, що визначає склад її технічних засобів і систем, приведена на рис. 2.1.

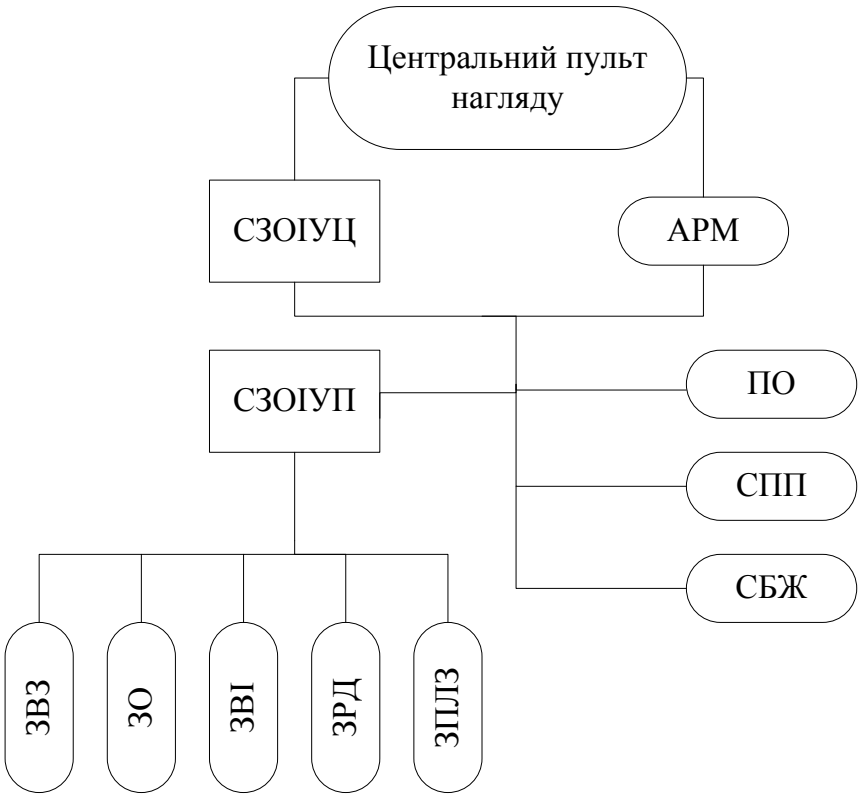


Рисунок 2.1 – Узагальнена структурна схема комплексної системи безпеки

З огляду на важливість кожного елемента узагальненої структурної схеми, можна виділити три основні групи ТЗО, без яких неможлива реалізація системи безпеки: пристрої виявлення загроз, система збору та обробки інформації і управління, а також засоби, пов'язані з тим чи іншим способом передачі інформації про стан системи ПЗ каналах зв'язку, доведення її до споживача (користувачів системи, спеціальних служб і т.д.).

Перераховані засоби забезпечують вчасну та адекватну реакцію комплексної системи безпеки на виявлену подію.

Розглянемо більш детально склад і особливості деяких елементів структурної схеми.

Засоби виявлення загроз (ЗВЗ).

У загальному випадку являють собою елементи апаратури ТЗО, які виконують функцію реагування на зовнішній вплив. наприклад, сейсмічне ЗВЗ реагує на коливання грунту, викликане рухом одухотвореного (людини, тварини) або неживого (автомобіля, трактора) предмета. Основу

функціонування ЗВЗ становить фізичний принцип дії його чутливого елемента (наприклад, електромагнітний, вібраційний, радіотехнічний, ємнісний, оптичний і т.д.).

Чутливий елемент – це первинний перетворювач, реагує на вплив на нього (пряме чи непряме) об'єкта виявлення і сприймає зміну стану навколишнього середовища.

Засіб виявлення – це пристрій, призначений для автоматичного формування сигналу з заданими параметрами (сигналу тривоги, інакше – сигналу спрацьовування або оповіщення) внаслідок вторгнення або подолання об'єктом виявлення чутливої зони (інакше – зони виявлення) даного пристрою [9].

В області забезпечення протівокрімінальной захисту нормативні документи оперують поняттям засіб виявлення проникнення і визначають його для охоронної і тривожної сигналізації як автоматичні і неавтоматичні (тривожна сигналізація) охоронні сенсори.

Сенсор (технічний засіб виявлення) - це пристрій для формування сповіщення про тривогу при проникненні (спробі проникнення) або ініціювання сигналу тривоги споживачем .

Виходячи із загальної структури комплексної системи безпеки, в кожній з підсистем технічних засобів можна виділити ті пристрої, які є засобами виявлення різних загроз і діють на основі аналізу тих чи інших фізичних параметрів контрольованого об'єкта (в залежності від призначення і виконуваних функцій підсистеми). До засобів виявлення загроз відносяться такі пристрої:

1. Для систем охоронної і тривожної сигналізації – охоронні і тривожні сенсори, що формують сигнали при різних видах несанкціонованого проникнення в захищені зони.

Формування сповіщення про тривогу відбувається при виявленні

– сенсорами наступних дій:

– рух або присутність об'єкта в контрольованій зоні;

– руйнування будь-яких конструкцій: скла, стін і т. д.;

– зміщення предметів, рам, дверей і т. д.;

– перетин контрольованої зони та ін.

2. Для відеонагляду – пристрої спостереження (відеокамери), що дозволяють візуально стежити за станом об'єкту, що охороняється в різних умовах: вдень під час нормальної роботи об'єкта (наприклад, магазину) фіксувати ситуацію під час нападу на об'єкт, вночі в період охорони реєструвати зміни в зображенні і попереджати про це.

3. Чинним стандартом відеокамера визначається як з точки зору фізичного принципу дії її чутливого елемента, так і з точки зору її становища в структурі сигналізації. Відеокамера є первинним джерелом відеосигналу в складі системи охоронної сигналізації [12].

4. Для пожежної сигналізації – пожежні сенсори, які являють собою сенсори виявлення загоряння і надсилають сигнали при появі ознак пожежі (при підвищенні температури вище допустимої, при збільшенні концентрації диму і т.п.) .

5. Для систем контролю та управління доступом – приймальні пристрої ідентифікації доступу, в якості яких використовуються кодонабірні пристрї (Клавіатури), для яких рішення про доступ приймається при введенні правильного коду, а також зчитувачі, які розшифровують інформацію, записану на ідентифікаторах різного типу і встановлюють права людей, майна, транспорту на переміщення в зоні, що під охороною. Для підвищення рівня безпеки контролю доступу може використовуватися подвійна технологія, що припускає спільне використання клавіатури для введення PIN -коду і зчитувача будь-якого типу (в залежності від необхідного рівня забезпечення безпеки і фінансових або організаційних обмежень). В цьому випадку код служить для підтвердження факту санкціонованого використання ідентифікатора.

6. Для систем захисту інформації – сенсори виявлення витоку інформації, що видають сигнал про спроби несанкціонованого отримання

інформації з об'єкта захисту. Це можуть бути передавачі підслуховуючих пристроїв, встановлені в приміщенні або підключені до телефонної лінії; визначники підключення до телефонної лінії та ін.

7. Для систем життєзабезпечення – сенсори контролю навколишнього середовища, що видають інформацію про стан середовища проживання людини, що дозволяють виявляти ситуації, небезпечні для життя або здоров'я людини, або попереджати про можливість виникнення такої ситуації (наприклад, витік газу, підвищення радіаційного фону або протікання). Прикладом можуть служити пристрої для контролю чистоти повітря в вентиляційних системах, дозиметри для виявлення підвищення радіаційного фону.

Сенсори контролю стану системи безпеки , які контролюють стан і працездатність системи і формують тривожні сигнали при порушення режиму роботи або спроби втручання в елементи системи для виведення її з ладу. При цьому система повинна постійно контролювати свою працездатність (здійснювати самоконтроль), повідомляти про несправності і охороняти себе від спроб несанкціонованого втручання (наприклад, від спроб відкрити корпус сенсора або заблокувати його).

Засоби оповіщення (ЗО).

Засоби оповіщення про тривогу – це технічні засоби, призначені для світлового та/або звукового оповіщення людей про виникненні небезпеки. Поширеними засобами оповіщення і зв'язку є засоби світло-звукової індикації (сирена, дзвінок, світлові-маячки), телефонний зв'язок, радіозв'язок, гучний зв'язок, що видає мовні повідомлення на різних мовах, телефакси, мобільні телефони, пейджери, переговорні пристрої , пневмопочта.

Комплекс засобів оповіщення формує систему оповіщення, яка спільно з системою зв'язку вирішує завдання оперативного управління та координації дій персоналу об'єкта в разі загрози, а також одночасного доведення до великого числа користувачів мовних повідомлень, звукових і/або світлових сигналів.

Системи оповіщення і зв'язку призначені для виконання наступних функцій:

– доведення достовірної, безперебійної службової інформації про обстановці на об'єкті і в його контрольних зонах до служб охорони при виникненні нештатної ситуації або загрозу їх виникнення;

– оповіщення осіб, санкціоновано знаходяться на об'єкті, що охороняється об'єкті, про аварійну ситуацію;

– привернення уваги оточуючих або поліції до охоронюваного об'єкту при спробі проникнення або крадіжки (наприклад, включення звукового сигналу автомашини і миготіння фар при проникненні в неї), пожежі або в інших ситуаціях;

– оперативна і одночасна передача розпоряджень ПЗ діям персоналу в

Засоби відображення інформації (ЗВІ).

Пристрої відображення інформації дозволяють спостерігати стан захищається, зміни в роботі ТЗО, що входять до складу комплексної системи безпеки.

Найпростіші ЗВІ є індикаторні лампи і світлодіоди, колір або режим роботи яких відповідає певному об'єкту або його станом. Це може бути рідкокристалічний дисплей контрольної панелі або клавіатури, на якому відображається відповідний текст, наприклад: набраний код доступу, номер відеокамери, в полі зору якої виявлено рух, назва або номер порушеної зони охорони, статус сигналізації (постановка на охорону, зняття з охорони, тривога і т.п.).

У більш складних системах це може бути монітор, на екрані якого відображається план об'єкту, що охороняється і його стан. Як пристрої виведення відеозображення в відеонагляді використовуються аналогові або рідкокристалічні відеомонітори, для яких встановлені вимоги до розміру діагоналі (не менше 17 дюймів) і робочому дозволу екрану (не нижче 1280х1024 точок або 960х768 ТВЛ).

Таким чином, ЗВІ в складі комплексної системи безпеки дозволяють спостерігати наступне:

– склад і стан об'єкту, що охороняється (наприклад, план об'єкта, які частини об'єкта охороняються, які ні, де і яке відбулося порушення);

– склад і стан всієї системи безпеки і її елементів (наприклад, кількість і стан шлейфів сигналізації, параметри системи, відповідні її нормальному функціонуванню або відхилень від норми, несправності, збої ПЗ та електроживлення).

2.3 Загальні принципи побудови систем безпеки

Розглянемо принципи побудови системи безпеки об'єкта, на основі яких встановлюються вимоги до створення та організації функціонування таких систем в цілому і складових її технічних засобів. При побудові захисту спеціального об'єкта необхідно керуватися такими принципами:

1. Адекватність прийнятим моделям загроз (розроблені організаційні та адміністративні заходи, технічні засоби захисту об'єктів і їх елементів повинні відповідати прийнятим загрозам і моделям порушників).

2. Зональна побудова або зональним принципом (системи безпеки повинна передбачати організацію та створення зон обмеженого доступу, що забезпечують "багаторівневий" захист об'єктів під охороною і їх критичних елементів).

3. Повинен бути забезпечений необхідний рівень ефективності для всіх типів порушників і способів вчинення злочинних дій.

4. Адаптивність (системи безпеки не повинна створювати перешкод функціонуванню об'єкта і повинна адаптуватися до технологічних особливостям його роботи, в тому числі в надзвичайних ситуаціях з урахуванням прийнятих на об'єкті заходів технологічної та пожежної безпеки).

Дотримання принципів побудови системи безпеки дозволяє забезпечити ефективність захисту об'єктів, яка визначається здатністю технічних підсистем комплексним і інтегрованим системам безпеки протистояти нештатним ситуаціям на об'єкті з урахуванням виявлених загроз і моделей порушників.

Розглянемо більш докладно зональний принцип побудови системи безпеки, який дозволяє раціонально зробити вибір і розподіл технічних засобів підсистем для охорони об'єкта і його критичних зон.

Під критичними зонами (елементами) об'єкта розуміють приміщення, їх конструктивні елементи, ділянки, реалізація загрози в відношенні яких може привести до найбільш суттєвих втрат. Для своєчасного виявлення і нейтралізації потенційних загроз необхідно визначити послідовні зони (або рубежі) забезпечення безпеки з одночасним виявленням загроз ПЗ кожній конкретній зоні.

У загальному випадку зона під охороною може бути визначена як частина об'єкту, що охороняється, контрольована одним шлейфом охоронної сигналізації (для комплексів охоронної сигналізації), одним шлейфом пожежної сигналізації (для установок пожежної сигналізації), одним шлейфом охоронно-пожежної сигналізації або сукупністю шлейфів охоронної та пожежної сигналізації (для омплексів охоронно-пожежної сигналізації) та до якої може бути обмежений доступ.

Шлейф сигналізації – це коло (електричне, радіоканальне, оптоволоконне або інше), що з'єднує вихідні вузли сенсорів, що включає в себе допоміжні (виносні) елементи і з'єднувальні лінії і призначена для передачі на прилад приймально-контрольний або на пристрій об'єктове системи передачі повідомлень інформації від сенсорів про контрольовані ними параметрах, а в деяких випадках – для подачі електроживлення на сенсори.

Рубіж охоронної сигналізації – це шлейф або сукупність шлейфів, контролюючих охоронювані зони території, будівлі або приміщення

(периметр, обсяг або площа, самі цінності або підходи до них) на шляху можливого руху порушника до матеріальних цінностям, при подоланні яких видається відповідне повідомлення про проникнення.

Під кордоном охорони розуміється сукупність охоронюваних зон, контрольованих кордоном сигналізації [12]. При організації зонування об'єкта повинно забезпечуватися посилення захисту від периферії до центру, тобто до критичних елементів, визначальним категорію об'єкта. Якщо при оцінці ефективності системи безпеки з'ясовується, що існуючих охоронюваних зон недостатньо для нейтралізації потенційних загроз, то можуть організовуватися додаткові рубежі захисту всередині існуючих зон.

Основу планування і технічного оснащення зон безпеки складає принцип рівнозахищенності їх кордонів. Наприклад, якщо при обладнанні зони периметра будівлі на одному з вікон першого поверху не буде металевої решітки або її конструкція ненадійна, то міцність і надійність інших решіток вікон цього поверху не мають ніякого значення, так як зона буде досить легко і швидко подолана порушником через незахищене (або слабо захищене) вікно. Отже, кордони зон безпеки не повинні мати незахищених ділянок.

Властивість адаптивності системи безпеки дозволяє своєчасно і гнучко враховувати динаміку потенційних і реальних загроз і небезпек об'єкту.

Таким чином, технічна підсистема комплексної інтегрованої системи безпеки повинна володіти адекватністю ПЗ відношенню до спектру загроз і небезпек об'єкту з урахуванням контрольних зон в своїй підконтрольній області та адаптивністю до змін умов функціонування об'єкта.

2.4 Зони забезпечення безпеки

Визначення послідовних рубежів (або захисних зон) з одночасним виявленням загроз ПЗ кожній конкретній зоні дозволяє вибрати технічні засоби забезпечення безпеки для найбільш ефективного вирішення завдань охорони об'єкта.

Такі рубежі (або зони безпеки) повинні розташовуватися послідовно – в загальному випадку, від огорожі навколо території об'єкта до критичних елементів об'єкта, таких як сейфи, сховища цінностей та інформації, вибухонебезпечних матеріалів, зброї тощо (Рис. 2.2). Чим складніше і надійніше захист кожної зони безпеки, тим більше часу буде потрібно порушнику на її подолання і тим більше ймовірність того, що розташовані в зонах ЗВЗ подадуть сигнал тривоги. Отже, у служби охорони буде більше часу для визначення причин тривоги і організації ефективної протидії загрозам [3].

Початковою зоною забезпечення безпеки є прилегла територія. Вона не є частиною об'єкта і може використовуватися порушниками для підготовчих робіт ПЗ організації несанкціонованих дій, наприклад, для спостереження і вивчення режиму охорони об'єкта і його охоронних структур. Тому прилегла територія також може розглядатися як зона забезпечення безпеки і контролюватися, в першу чергу, засобами відеонагляду.

Першою зоною є зовнішній периметр території об'єкта охорони. загрози: подолання периметральних коштів інженерно технічної укріпленості (в тому числі їх руйнування) для проникнення на територію з метою вторгнення на об'єкт. У першій зоні можуть використовуватися засоби інженерно-технічної укріпленості (загородження, паркани), відеонагляду, засоби периметральної захисту в складі системи охоронної сигналізації, а також фізична охорона, тобто працівники власної служби безпеки або співробітники позавідомчої охорони.

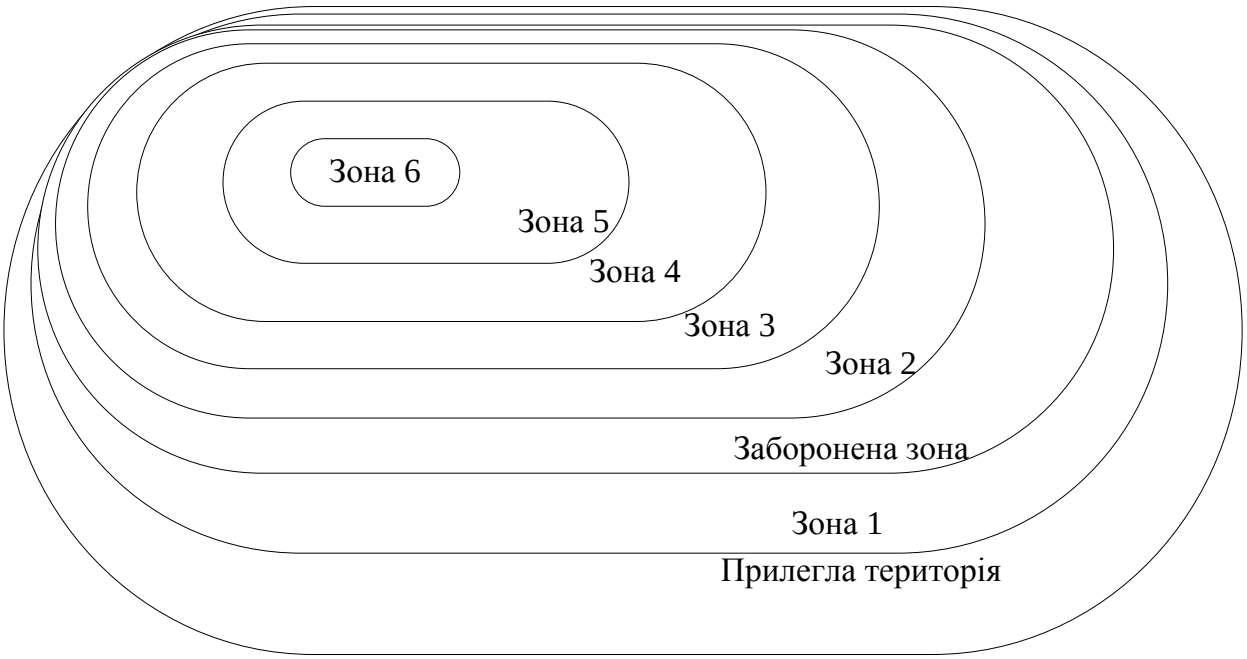


Рисунок 2.2 – Розташування зон забезпечення безпеки

Заборонена зона (або зона відторгнення) при необхідності організовується уздовж основного огорожі периметра з внутрішньої сторони території об'єкта і призначена для розміщення на ній ТЗО і виконання службових завдань особовим складом підрозділів охорони. Заборонена зона повинна бути ретельно спланована і розчищена. В ній не повинно бути ніяких будівель, предметів і рослинності, ускладнюють застосування ТЗО і дії сил охорони. заборонена зона може бути використана для організації охорони об'єкта за допомогою сторожових собак. Для забезпечення нормальної роботи ТЗО на відкритих майданчиках та периметрів об'єктів ширина забороненої зони повинна перевищувати ширину їх зони виявлення.

Друга зона охорони включає в себе територію, на якій знаходиться об'єкт, що охороняється. Загрози: несанкціоноване проникнення на територію з метою подальшого вторгнення на об'єкт.

При захисті даної зони використовується комплекс заходів, що складається з технічних засобів відеонагляду і охоронно-пожежної сигналізації (ОПС).

Третю зону охорони становить елементи периметра об'єкту, що охороняється, будівлі або приміщення:

– будівельні конструкції ПЗ периметру будівлі або приміщень об'єкта, тобто всі віконні і дверні прорізи;

– місця введення комунікацій, вентиляційні канали;

– виходи до пожежних драбин;

– несучі та ненесучі стіни;

– вентиляційні короба, димоходи.

Загрози: несанкціоноване проникнення в будівлю через слабко укріплені, незаблоковані засобами сигналізації ділянки, а також підготовчі роботи для подолання технічних засобів забезпечення безпеки.

Ця зона контролюється засобами відеонагляду, ОПС і фізичної охорони.

Четверта зона внутрішні обсяги приміщень об'єкта.

За допомогою технічних засобів системи контролю та управління доступом в четвертій зоні повинні бути організовані пропускний режими.

Для цього виконується поділ об'єкта на три основні зони доступу [11]:

– перша зона (зона вільного доступу) – будівлі, території, приміщення, доступ до яких персоналу, відвідувачам і особам, які проживають на об'єкті, не обмежений;

– друга зона (зона обмеженого за часом або рівню пріоритету доступу) – приміщення, доступ до яких дозволений в обмежений час (наприклад, покупцям магазину в робочі години, персоналу – відповідно до режиму роботи) або обмеженому складу персоналу, а також відвідувачам об'єкта за разовими перепустками або в супроводі персоналу об'єкта;

– третя зона спеціальні приміщення об'єкта, доступ до яких мають строго певні співробітники і керівники (наприклад, приміщення керівництва об'єкта і охорони), а також приміщення безпосереднього зосередження і зберігання матеріальних та інших цінностей.

Пропуск користувачів на об'єкт через пункти контролю доступу повинен здійснюватися:

– в першій зоні доступу за однією ознакою ідентифікації;

– у другій зоні доступу за двома ознаками ідентифікації (Наприклад, електронна картка і ключ від механічного замка);

– в третій зоні доступу не менше, ніж за двома ознаками ідентифікації.

Загрози: несанкціоноване проникнення в приміщення з матеріальними і фінансовими ресурсами; виведення з ладу засобів відеонагляду і ОПС; установка підслуховуючих та інших пристроїв знімання інформації; нейтралізація працівників охорони або служб безпеки для подальшого нападу на касирів з метою заволодіння грошовими засобами або іншими матеріальними або фінансовими ресурсами; захоплення заручників; проникнення в комп'ютерну мережу підприємства з злочинними цілями; фізичне знищення керівників об'єкта з метою розвалу підприємства як конкурента; напад на співробітників охорони для вчинення терористичних або інших актів; розкрадання, крадіжка з місць безпосереднього зберігання цінностей.

Ці зони контролюються технічними засобами ОПС, систмами контролю та управління доступом, відеонагляду спільно із засобами захисту інформації (СЗІ), фізичної охороною.

П'ята зона окремі предмети, наприклад сейфи, картини, скульптури і підходи до них.

Загрози: розкрадання, акти вандалізму. Для захисту використовується відповідні технічні засоби охоронної сигналізації та відеонагляду.

Шоста зона – власне система безпеки. Включає в себе захист технічних і програмних засобів забезпечення безпеки.

Загрози: несанкціонований доступ до елементів системи безпеки з метою або повного виведення її з ладу, або блокування окремих елементів, що робить неможливим виконання ними основних функцій при зовнішньому збереженні працездатності.

Для запобігання загрозам використовуються сенсори розтину корпусів і зняття зі стіни, самодіагностика елементів системи, пристрої виявлення блокування сенсорів та ін.

Кожна з зон може включати в себе кілька рубежів охорони в залежності від значимості об'єкта або його критичних елементів, контрольованих даної зоною. При цьому критична зона (наприклад, область безпосереднього зберігання матеріальних цінностей) повинна знаходитися в центрі, і для підходу до неї необхідно подолання всіх зон і рубежів охорони [1, 9].

2.5 Умови функціонування систем безпеки

Пріоритетними для кожної системи безпеки є вимоги, забезпечують безпеку для життя людей, і пожежну безпеку об'єкта. Тому основним технічним вимогою до них є забезпечення необхідної функціональної і апаратної надійності, пожежної безпеки та завадостійкості. Під надійністю розуміється її властивість виявляти із заданою вірогідністю проникнення (спробу проникнення) на об'єкт, що охороняється (зону об'єкта).

Основні умови функціонування системи безпеки можуть бути сформульовані наступним чином [1, 12].

1. Жодна з підсистем у її складі не повинна порушувати режим функціонування об'єкта, а саме: функції спільно діючих систем повинні доповнювати один одного, не заважаючи працездатність інших складових частин.

2. Система безпеки повинна управлятися як централізовано, так і децентралізовано з контролем рівня доступу персоналу до системи.

3. Система безпеки повинна зберігати справний стан при впливі факторів навколишнього середовища і відновлювати працездатне стан після закінчення їх дії.

4. Системи безпеки не повинна виходити з ладу при відключенні електроенергії на об'єкті і зберігати працездатний стан при відключенні

мережевого або іншого основного джерела електроживлення впродовж часу переривання електроживлення. Сигналізації не повинні видавати помилкових тривог при перемиканні джерел електроживлення з основного на резервний і назад.

5. Всі події, що відбуваються в системі, повинні протоколюватися.

6. Система повинна контролювати, тестувати і захищати себе від несанкціонованого доступу до управління.

7. Спільно діючі об'єктові системи різного функціонального призначення вимагають різного реагування на видані ними сигнали аварії, тривоги.

8. Система не повинна створювати загроз об'єкту забезпечення безпеки.

2.6 Принципи організації інтегрованих системи безпеки

Конкретний склад функціональних блоків інтегрованих системи безпеки визначають при цільової розробці відповідно до технічного завдання.

При цьому структура підсистем, елементи яких взаємодіють (інтегруються) між собою, визначається рівнем інтеграції, на якому це взаємодія відбувається.

За функціональним призначенням можна виділити такі рівні (рис.2.3) взаємодії елементів інтегрованих підсистем безпеки [6, 10].

Вищий (глобальний) рівень передбачає взаємодію інтегрованих системи безпеки з іншими інформаційними системами, являє собою комп'ютерну мережу типу «клієнт/сервер» на основі мережі Ethernet, з протоколом обміну TCP/IP і використанням мережевих операційних систем (ОС) професійного класу типу Windows або Linux. Цей рівень забезпечує зв'язок між сервером і робочими станціями операторів, тут забезпечується управління інтегрованою системою безпеки з використанням програмного забезпечення. На даному рівні необхідна висока надійність і захист від несанкціонованого доступу.

Перший (системний) рівень передбачає інформаційне взаємодія СЗОІУ окремих підсистеми безпеки і підсистем протидії та ліквідації загроз в межах інтегрованої системи безпеки (це можуть бути приймально-контрольні прилади, що забезпечують управління засобами ОПС та контролери). На даному рівні СЗОІУЦ або центральний процесор (сервер) об'єднує всі підсистеми.

Другий (системний) рівень передбачає інтеграцію локальних (Або периферійних) систем збору і обробки інформації окремих підсистеми безпеки. Інтеграція може здійснюватися завдяки ПЗ по каналах зв'язку або через інтерфейси інтеграції периферійних систем обробки (ІІПСО). В цьомувипадку можливе поєднання вертикальної інтеграції (зв'язок між контролерами і комп'ютерами підсистем) і горизонтальної інтеграції (зв'язок між однорідними контролерами в кожній з підсистем) на вертикальному рівні найбільш часто використовується інтерфейс RS-232, на горизонтальному рівні RS-485, призначені для побудови мереж промислового рівня з хорошою завадостійкістю і достатньою швидкістю обміну даними.

Третій (модульний) рівень передбачає взаємодію між СЗОІУП і ЗВЗ своїх підсистем. Контролери «місцевого» значення керують невеликою групою сенсорів, відеокамер, зчитувачів, виконавчих пристроїв і т.п. Тут, як правило, застосовуються інтерфейси RS-485, RS-232 або стандартні інтерфейси зчитувачів Wigand 26. На цьому рівні розташовуються також засоби управління оповіщенням, пожежогасіння і протипожежної автоматикою, адресні блоки управління з релейними і потенційними виходами [6, 10].

Четвертий (нижній) рівень передбачає взаємодію ЗВЗ різних підсистемах безпеки через узагальнені шлейфи або відповідні інтерфейси інтеграції пристроїв виявлення (ІІППВ).

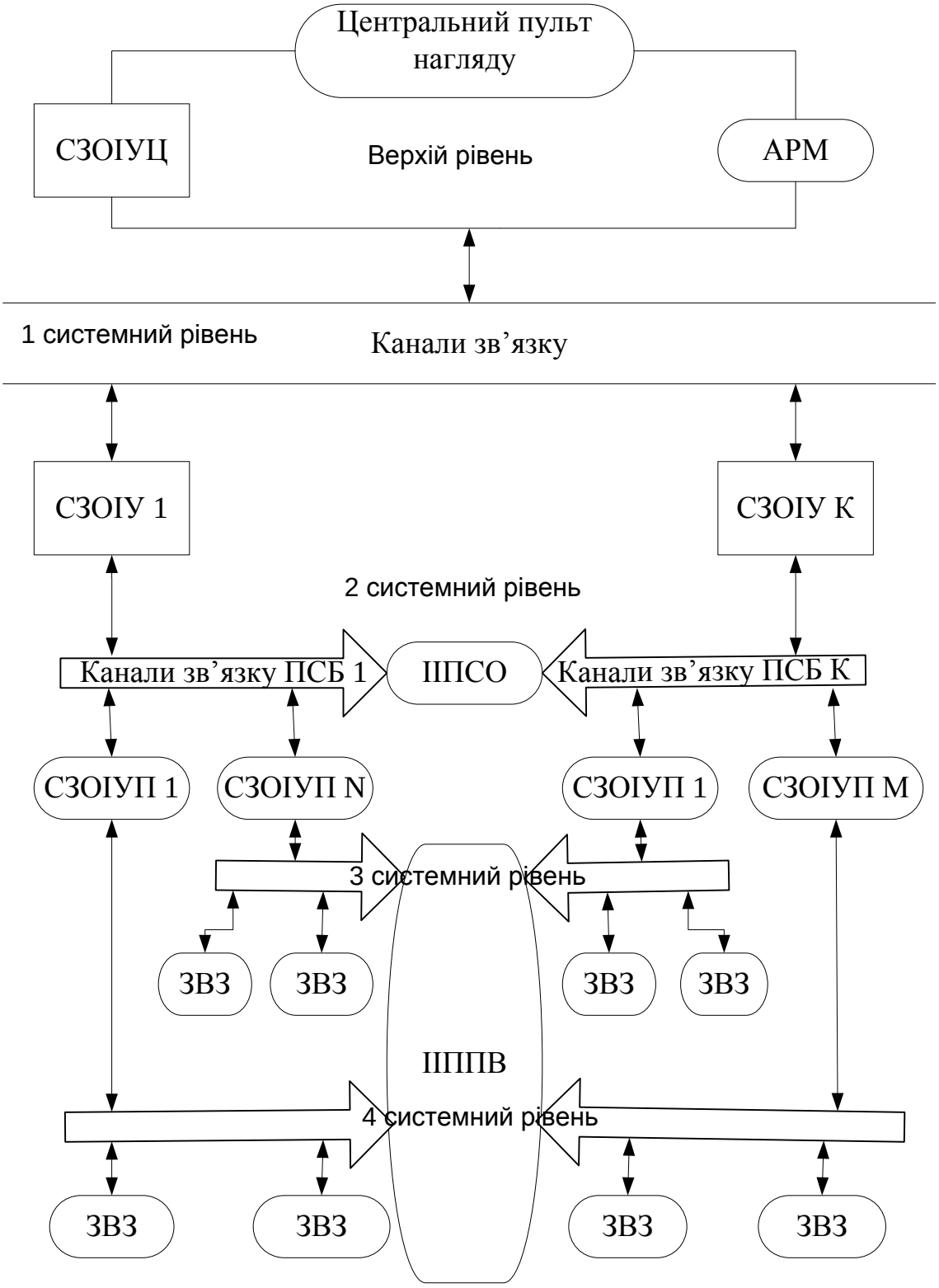


Рисунок 2.3 – Рівні інтеграції різних елементів інтегрованої комплексної системи безпеки.

2.7 Системи охоронної, тривожної та пожежної сигналізації

2.7.1 Структурна схема охоронно-пожежної сигналізації

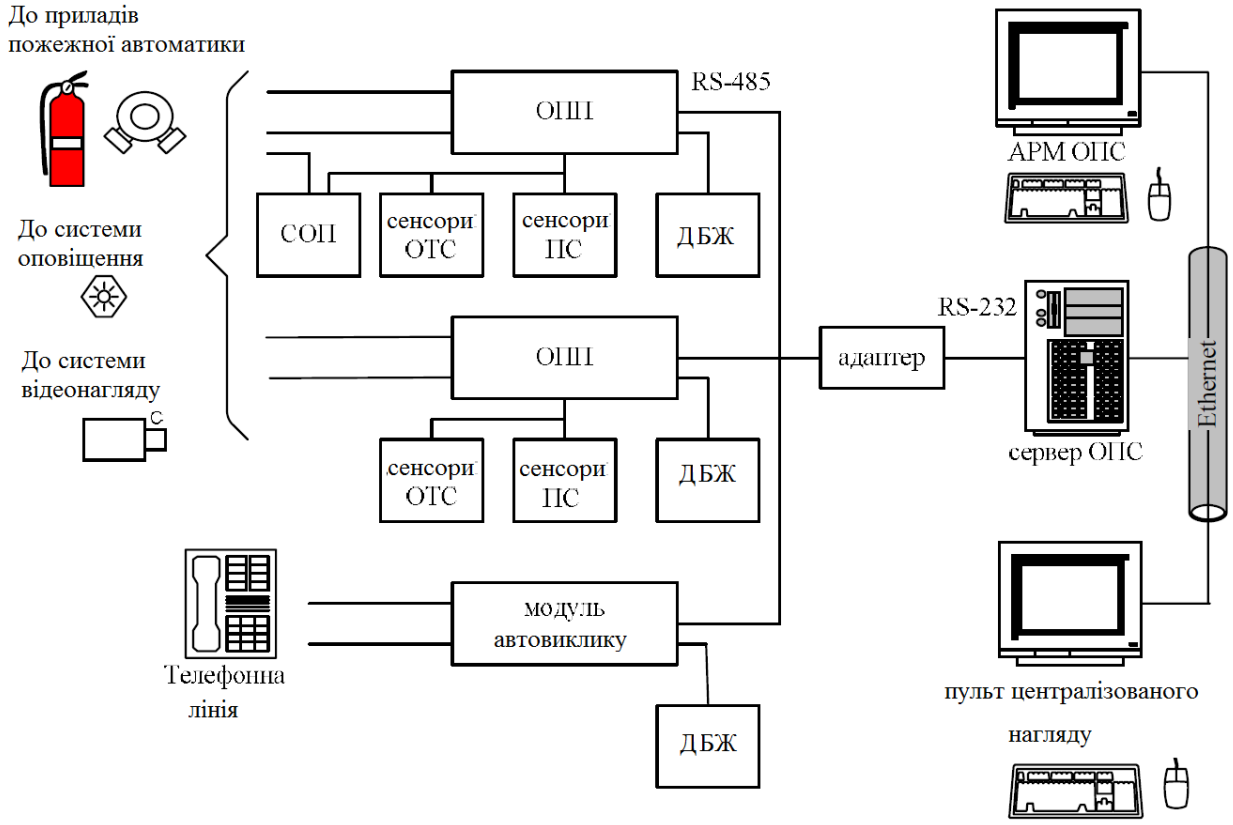


Рисунок 2.6 – Структурна схема охоронно-пожежної сигналізації: ОПП – охоронно-пожежна панель; АРМ – автоматизоване робоче місце; ОТС – охоронно-тривожна сигналізація; ПС – пожежна сигналізація; СОП – система охорони периметра; ДБЖ – джерело безперебійного живлення.

Кожен тип сенсора має свій перелік основних технічних характеристик, що визначаються відповідними стандартами. У той же час, навіть однотипні сенсори мають відмінності в конструктивних особливості складових частин, зручність експлуатації, надійності, рівні дизайну, що враховується при виборі того чи іншого сенсора або фірми-виробника.

2.7.2 Засоби виявлення загроз в складі ОПС

Сенсори охоронні (СО) розглянемо через функціональні особливості деяких активно застосовуваних на практиці охоронних сенсорів відповідно визначеннями, які дані в нормативних документах.

СО магнітогерконовий (рис. 2.7) формує повідомлення про тривогу при розмиканні магнітних контактів сенсора. Призначений для блокування різних будівельних конструкцій на відкриття (дверей, вікон, люків, воріт і т.п.).

Складається з герметизованого магнітокерованих контакту (геркона) і магніту в пластмасовому або металевому немагнітному корпусі. Магніт встановлюється на рухомий (відкривається) частини будівельної конструкції (полотні двері, стулки вікна і т.п.), а магнітоуправляємий контакт - на нерухомої частини (коробці двері, рами вікна і т.п.).

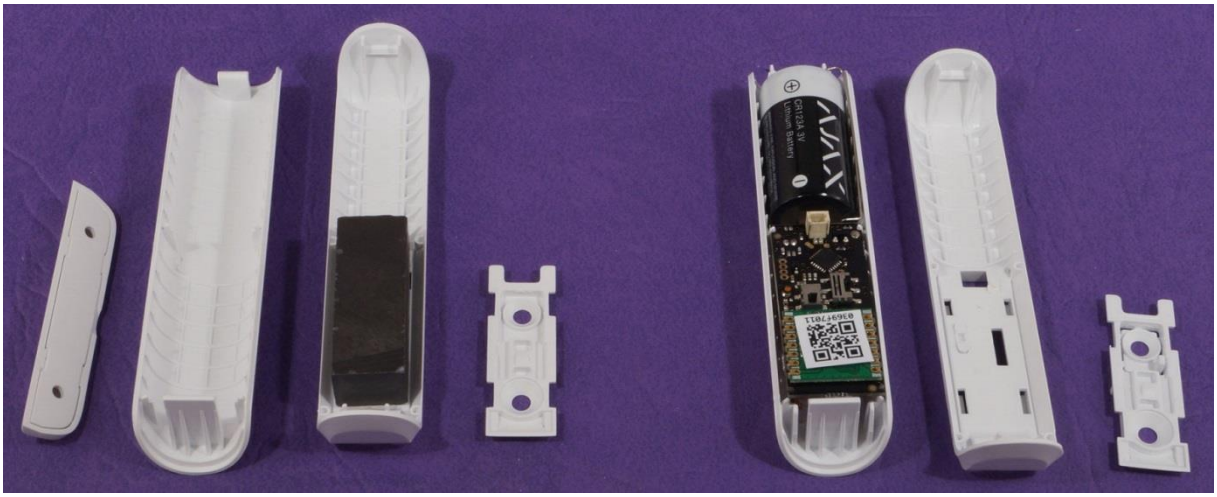


Рисунок 2.7 – Приклад моделі магнітоконтактного сенсора

СО ударно-контактний формує повідомлення про тривогу при ударному впливі об'єкта виявлення на контрольовану поверхню об'єкту, що охороняється. Призначений для блокування різних засклених конструкцій (вікон, вітрин, вітражів тощо) на розбиття.

Складається з блоку обробки сигналу і від 5 до 15 сенсорів розбиття скла. Місце розташування зазначених складових частин сенсора визначається

кількістю, взаємним розташуванням і площею заблокованих скляних полотен.

СО п'єзоелектричний формує повідомлення про тривогу при впливі пружних хвиль, що виникають в твердому тілі при фізичному впливі на нього (ударі з метою руйнування або розтину), яке виявляється п'єзоелектричним чутливим елементом.

Призначений для блокування будівельних конструкцій (стін, підлог, стель і т.п.) і окремих предметів (сейфів, металевих шаф, банкоматів і т.п.) на руйнування.

СО (охоронно-пожежний) оптико-електронний активний формує повідомлення про проникнення (спробі проникнення) або пожежі при нормованій зміні (припинення) відбиття потоку або припинення (зміни) прийнятого потоку енергії оптичного випромінювання сенсора, викликаного рухом порушника в зоні виявлення. Зона виявлення сенсорів має вигляд "променевого бар'єру ", утвореного одним або декількома розташованими в вертикальній площині паралельними вузьконаправленими променями. Зони виявлення різних сенсорів відрізняються довжиною і кількістю променів.

Конструктивно такі СО складаються з двох окремих блоків – блоку випромінювача і блоку приймача, рознесених на робочу відстань (дальність дії). Призначені для захисту внутрішніх і зовнішніх периметрів, вікон, вітрин і підступів до окремих предметів (сейфів, музейних експонатів і т.п.).

СО (охоронно-пожежний) оптико-електронний інфрачервоний пасивний (рис. 2.8) реагує на зміну рівня інфрачервоного випромінювання внаслідок переміщення людини в зоні виявлення. Дані сенсори найбільш широко поширені в охоронній практиці. За допомогою спеціально розроблених для них оптичних систем (лінз Френеля) можна просто і швидко отримувати зони виявлення різних форм і розмірів і використовувати їх для захисту приміщень будь-якої конфігурації.

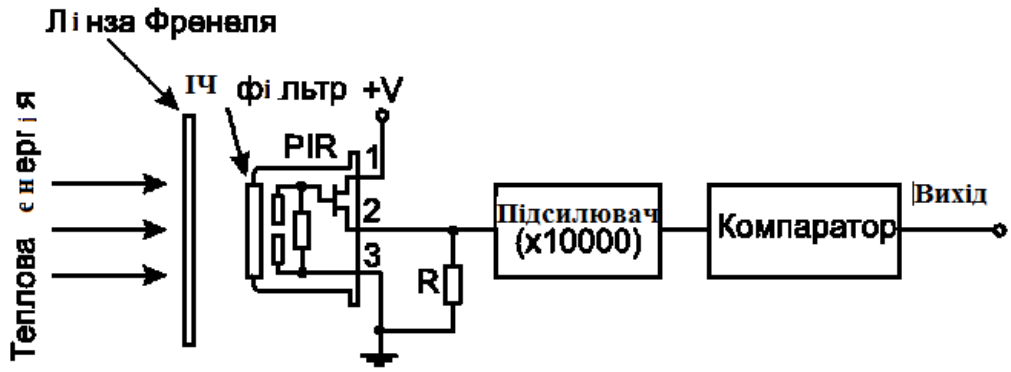


Рисунок 2.8 – Структурна схема проводового ІЧ сенсора руху

Сенсор реєструє різницю між потоками інфрачервоного випромінювання, що виходять від тіла людини і фону (під фоном розуміється поверхню стін, підлоги, стелі та інших предметів в зоні виявлення ІВ).

Чутливим елементом є піроелектричний перетворювач (піропріемніка), на якому фокусується інфрачервоне випромінювання за допомогою дзеркальної або лінзи оптичної системи (Останні найбільш широко поширені).

Зона виявлення сенсора є просторовою, що складається з елементарних чутливих зон в вигляді променів, розташованих в один або кілька ярусів або в вигляді тонких і широких пластин, розташованих у вертикальній площині. Умовно зони виявлення сенсорів можна розділити на кілька видів: одноярусна типу "віяло"; багатоярусна; вузьконаправлена типу "завіса", вузьконаправлена типу "променевий бар'єр"; панорамна багатоярусна та інші [12].

СО ємнісний формує повідомлення про тривогу при зміні ємності його чутливого елемента (антени), яке може бути обумовлено наближенням людини до об'єкта охорони або його дотиком до охоронюваного предмету.

При цьому об'єкт, що охороняється предмет повинен встановлюватися на підлозі з хорошим ізоляційним покриттям або на ізолюючої прокладки.

Ємнісні сенсори призначені для блокування металевих шаф, сейфів, окремих предметів, створення захисних загороджень.

СО акустичний (рис. 2.9) призначений для дистанційного виявлення руйнування скляного листа шляхом реєстрації звукових коливань в приміщенні, що генеруються склом при його руйнуванні під впливом механічного удару, і для формування сповіщення про тривогу [3, 11].

Застосовується для блокування засклених конструкцій (вікон, вітрин, вітражів тощо) на розбиття. при установці сенсора всі ділянки, що охороняється заскленої конструкції повинні бути в межах його прямого огляду.

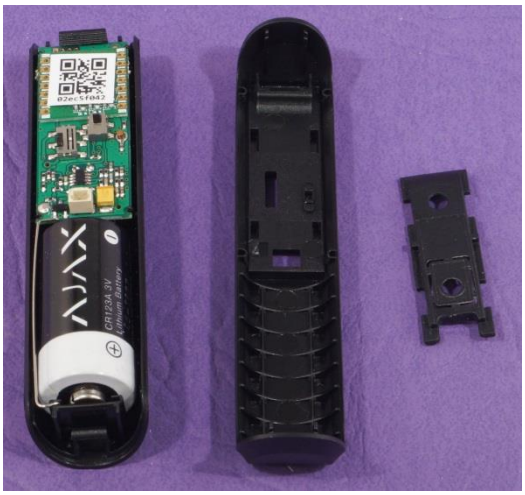


Рисунок 2.9 – Приклад моделі безпроводового акустичного сенсора

СО охоронно-пожежний ультразвукової формує повідомлення про проникнення (спробі проникнення) або пожежі (загорянні) при впливі на поле акустичних хвиль ультразвукового діапазону, випромінюваних сенсором, ознак появи людини або пожежі в зоні виявлення. Призначений для блокування обсягів закритих приміщень. Зона виявлення має форму еліпсоїда обертання або каплевидную форму. Через низку перешкодостійкість і складності експлуатації в даний час майже не використовуються.

СО радіохвильовий (рис 2.10) формує повідомлення про проникнення (спробі проникнення) при нормованому обурення поля електромагнітних хвиль надвисокочастотного діапазону в його зоні виявлення.

Призначений для захисту обсягів закритих приміщень, внутрішніх і зовнішніх периметрів, окремих предметів і будівельних конструкцій, відкритих майданчиків. Зона виявлення також має форму еліпсоїда обертання або каплевидную форму і для різних сенсорів різниться тільки розмірами.

Розрізняють одно- і двохпозиційні СО.

Однопозиційні застосовують для захисту обсягів закритих приміщень і відкритих майданчиків. Двопозиційні - для захисту периметрів.

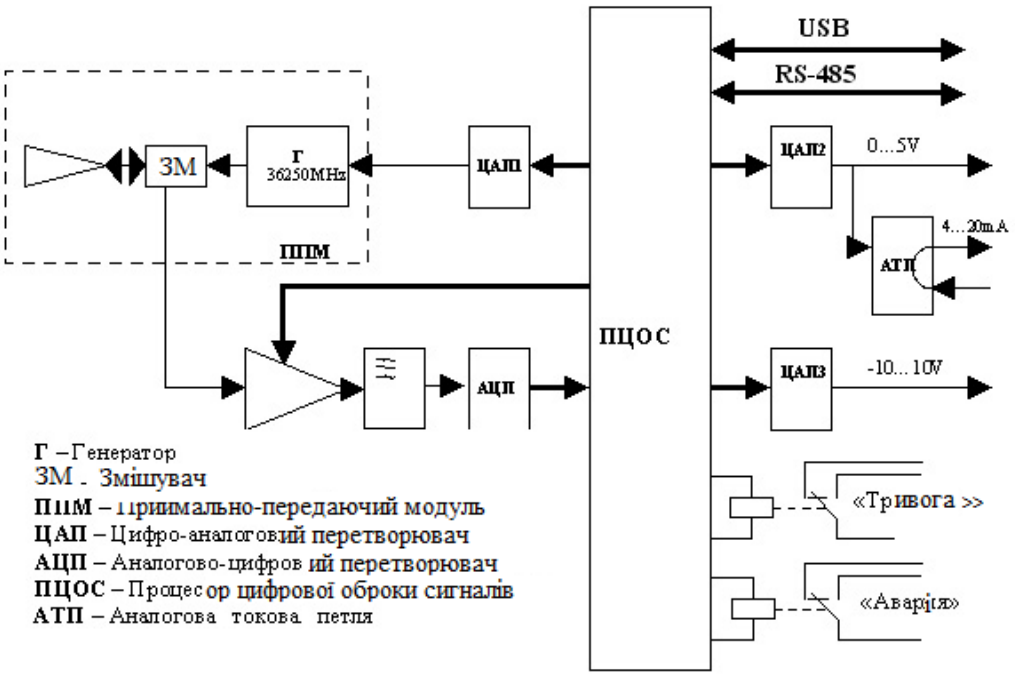


Рисунок 2.10 – Структурна схема радіохвильового сенсора руху

СО комбінований (рис 2.11) дозволяє виявити об'єкт виявлення на основі використання двох і більше різних фізичних принципів дії, при цьому поєднуються зони виявлення за цими принципами.

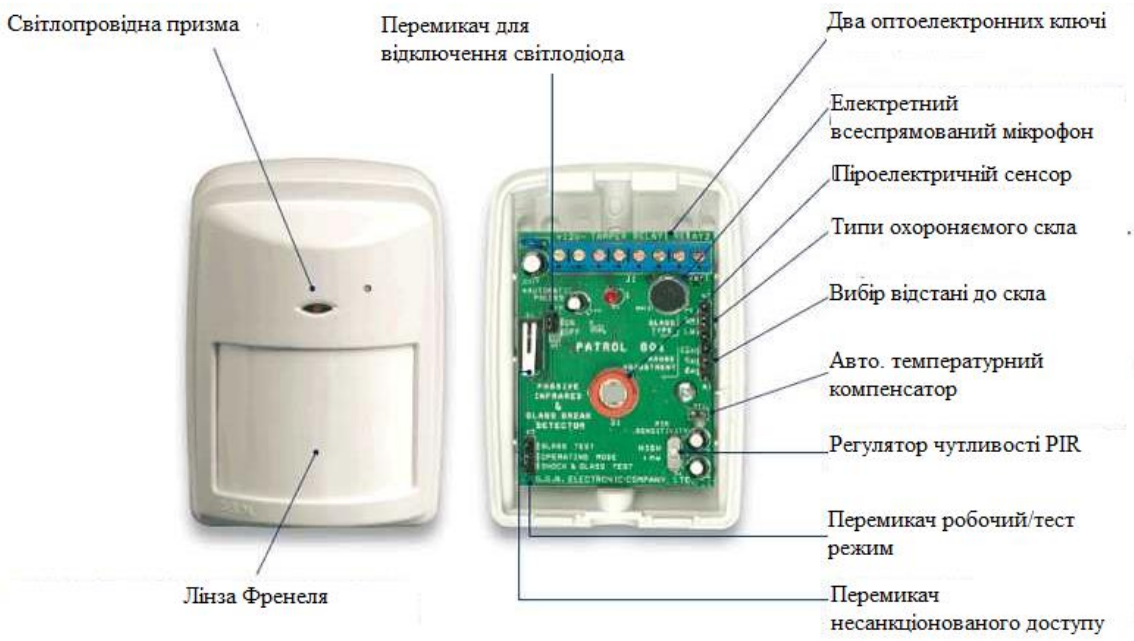


Рисунок 2.11 – Приклад моделі безпроводового комбінованого сенсора

СО суміщений формує повідомлення про тривогу при різних видах фізичного впливу об'єкта виявлення. Являє собою два СО, побудованих на різних фізичних принципах виявлення, об'єднаних конструктивно в одному корпусі.

Сенсори тривожної сигналізації.

Сенсори тривожної сигналізації призначені для ручної або автоматичної подачі тривожного сповіщення на внутрішній пульт охорони об'єкта у випадках можливого злочинного нападу на співробітників, клієнтів або відвідувачів об'єкта.

2.7.3 Засоби збору, обробки, відображення інформації та управління

Як було зазначено раніше, апаратно-технічні засоби збору та обробки інформації та управління формують центральну і периферійні СЗОІУ, що входять до складу комплексних інтегрованих системи безпеки. Вони призначені для виконання безперервного збору інформації від сенсорів, формування і передачі повідомлень про стан об'єкта [2, 4], та контролю їх справності.

У зв'язку з цим засоби збору і обробки інформації повинні мати такі функціональні характеристики:

– інформаційна ємність – кількість контрольованих приладом зон безпеки;

– інформативність – кількість переданих (прийнятих) повідомлень на системи передачі сповіщень;

– час прийому повідомлення від сесорів (максимально допустимий час контролю всіх сенсорів, підключених до приладу);

– рівень захисту від несанкціонованого доступу до приладу при виконанні функцій взяття під охорону і зняття з охорони об'єкта;

– параметри завадостійкості лінії (каналу) зв'язку приладу з сенсорами;

– параметри і характеристики інтерфейсу каналу зв'язку приладу з засобами передавання тривожних сповіщень.

Прилади приймально-контрольні ППК в системах ОПС є проміжною ланкою між об'єктовими первинними засобами виявлення проникнення або пожежі (сенсорами) і СПП.

ППК охоронний (охоронно-пожежний) – це технічний засіб охоронної або охоронно-пожежної сигналізації для прийому сповіщень від сенсорів (шлейфів сигналізації) або інших приймально-контрольних приладів, перетворення сигналів, видачі повідомлень для безпосереднього сприйняття

людиною, подальшої передачі повідомлень та включення сенсорів, а в деяких випадках і для електроживлення охоронних сенсорів .

Прийнята така класифікація ППК охоронних [2, 4] .

1. ПЗ виду організації тривожної сигналізації на об'єкті розглядають ППК: автономні – призначені для забезпечення автономної сигналізації, при якій повідомлення про стан контрольованого об'єкта видаються тільки на звукові та світлові сенсори, встановлені на об'єкті, що охороняється або в безпосередній близькості до нього; локальні – призначені для забезпечення локальної сигналізації на об'єкті, при якій повідомлення про стан, а також управління контрольованим шлейфом (зонами) здійснюється з допомогою засобів відображення інформації та управління (індикаторні панелі, пульти), що входять до складу ППК; централізовані – призначені для централізованої сигналізації і роботи спільно або в складі СПП, при якій сповіщення з ППК передаються на ПЦС СПП за допомогою використання різних каналів зв'язку (телефонні лінії, радіоканали, виділені лінії і ін.).

2. За способом контролю сенсорів ППК поділяються на: безадресні (без реєстрації адреси сенсора) – прилади, мають тільки безадресні шлейфи сигналізації; адресні – прилади, що мають адресні шлейфи сигналізації; комбіновані – прилади, що мають безадресні і адресні шлейфи сигналізації.

3. За структурою шлейфу сигналізації розглядають ППК: зі шлейфами сигналізації радіальної структури; зі шлейфами сигналізації кільцевої структури (Магістральні); зі шлейфами сигналізації деревовидної структури; зі шлейфами сигналізації комбінованої структури.

4. ПЗ виду каналу зв'язку з сенсорами розглядають ППК: з дротяними каналами зв'язку; з безпроводовим (радіоканал або ін.) каналом зв'язку; з іншими каналами зв'язку (силова електромережа і т.д.).

5. За інформаційної ємності розглядають ППК: малої інформаційної ємності – до восьми шлейфів сигналізації (адрес); середньої інформаційної ємності – від дев'яти до 64 шлейфів сигналізації (адрес); великий інформаційної ємкості – понад 64 шлейфів сигналізації (адрес).

6. За інформативності розглядають ППК: малої інформативності – до восьми видів сповіщень; середньої інформативності – від дев'яти до 16 видів сповіщень; великий інформативності – понад 16 видів повідомлень.

ППК для локальної сигналізації повинні додатково до основних функцій забезпечувати: а) відображення за допомогою індикаторів, розташованих на приладі, виносному табло або пульті управління, стану ППК або кожного шлейфа сигналізації або адреси; б) звукову сигналізацію про тривогу за допомогою вбудованого або зовнішнього звукового оповіщувача.

ППК пожежний – технічний засіб, призначений для прийому сигналів від пожежних сенсорів, здійснення контролю цілісності шлейфа пожежної сигналізації, світлової індикації та звукової сигналізації подій, формування стартового імпульсу запуску приладу управління пожежного.

2.7.4 Технічні засоби оповіщення

Система оповіщення (СО) на об'єкті, що охороняється і його території створюється для оперативного інформування людей про виниклу або наближається позаштатної ситуації (аварії, пожежі, стихійного лихо, напад, терористичний акт) і координації їх дій.

Ооповіщувач – технічний засіб, призначений для оповіщення людей про пожежу за допомогою подачі світлового, звукового (рис. 2.12) або мовного сигналу.

Рисунок 2.12 – Приклад моделі домашньої сирени

2.7.5 Засоби передачі сповіщень

Системи передачі сповіщень (СПП) про проникнення і пожежі являє собою сукупність спільно діючих технічних засобів, призначених для контролю і управління територіально-розподіленими (розосередженими) об'єктами на відстані із застосуванням спеціальних перетворювачів сигналів для ефективного використання каналів зв'язку. При цьому в якості каналів передачі сповіщень використовуються лінії міської телефонної мережі або радіоканал.

СПП класифікуються за такими ознаками [12]:

1. За інформаційної ємності (кількості об'єктів, що охороняються) розглядають СПП: малої інформаційної ємності – до 200 номерів (адрес) на об'єктах, що охороняються; середньої інформаційної ємності – від 201 до 1000 номерів (адрес) на об'єктах, що охороняються; великий інформаційної ємкості – понад 1000 номерів (адрес) на об'єктах, що охороняються.

2. ПЗ можливості нарощування інформаційної ємкості – на системи з постійною інформаційною ємністю і з можливістю наращування інформаційної ємності.

3. За інформативності – на системи малої інформативності, середньої інформативності та великої інформативності

4. За типом використовуваних ліній (каналів) зв'язку: виділені канали (провідні, оптоволоконні або інші); лінії (канали) телефонної мережі загального користування, в тому числі перемикаються, зайняті телефонним зв'язком, з використанням частотного виділення службових сигналів, з використанням апаратури автоматичного набору номера (інформаторние); радіоканали спеціальних радіомереж відомчої приналежності або загального користування, в тому числі мереж стільникового зв'язку; комбіновані канали зв'язку.

5. ПЗ виду формату повідомлення.

6. За алгоритмом обслуговування об'єктів.

7. За способом відображення надходить на ПЦС інформації.

8. За кількістю напрямків передачі інформації.

Розглянемо детальніше лінії (канали) зв'язку:

1. Виділені канали (провідні, оптоволоконні або інші); - лінії (канали) телефонної мережі загального користування, в тому числі перемикаються, зайняті телефонним зв'язком, з використанням частотного виділення службових сигналів, з використанням апаратури автоматичного набору номера (інформаторние);

2. Зайняті лінії телефонного зв'язку. Нині виводяться з експлуатації.

3. Комутовані телефонні лінії. Передача інформації ПЗ телефонних лініях здійснюється за допомогою спеціалізованих модемів-комунікаторів ПЗ спеціалізованим протоколам: Contact ID , SIA Level 3, Fast Format і ін.

Система передачі сповіщень радіоканальні (РСПП) або СПП ПЗ радіочастотним каналах зв'язку застосовується для охорони нетелефонізованих об'єктів, від яких єдиним способом передачі інформації є

радіозв'язок, або як доповнення до телефонному каналу для підвищення надійності системи ОПС.

Залежно від типу використовуваного радіоканалу все РСПП можна розділити на три основні групи: РСПП, що використовують передачу сигналу в загальнодоступних частотних діапазонах (27, 433, 868 МГц); РСПП, що використовують передачу сигналу в виділених частотних діапазонах (136-174 МГц, 400-512 МГц, 30-52 МГц); системи моніторингу, що використовують в якості носія повідомлень стільниковий зв'язок стандарту GSM (GSM Voice, SMS, GPRS).

Основною перевагою РСПП на базі GSM є відсутність необхідності придбання частотного ресурсу і побудови мережі ретрансляторів, використання існуючих мереж ретрансляції, які забезпечують дальність дії в рамках зони покриття стільникового мережі операторів мобільного зв'язку.

Комбіновані (гібридні) СПП складаються з провідних та радіоканальних каналів СПП в різних поєднаннях. Комбіновані системи застосовуються для підвищення надійності передачі повідомлень від об'єкта охорони на ПЦС. Комбіновані системи мають більш високу вартість в порівнянні з системами на базі одного каналу.

Пульт централізованого спостереження спільно з СПП являє собою систему, призначену для збору інформації з об'єктів, обладнаних засобами ОПС, і передачі інформації про стан об'єктів на АРМ операторів пульта.

Склад обладнання ПЦС залежить від кількості і складу необхідних каналів зв'язку, кількості АРМ і інших чинників. У загальному випадку ПЦС складається з наступних елементів: приймач повідомлень від СПП; сервер збору, зберігання і обробки інформації; автоматизоване робоче місце оператора ПЦС; система зв'язку ПЦС з патрульними екіпажами.

Основними технічними характеристиками ПЦС є: інформаційна ємність (максимальна кількість абонентів); кількість і типи підтримуваних каналів прийому повідомлень (радіоканал, телефонний канал, мережа GSM , протокол TCP/IP та ін).

2.8 Аналіз побудови систем відеонагляду

Система відеонагляду – це телевізійна система закритого типу, призначена для отримання телевізійних зображень з об'єкту під охороною в цілях забезпечення захисту [2].

2.8.1 Призначення і склад систем відеонагляду

З урахуванням конкретних умов і особливостей процесів діяльності на об'єкті система відеонагляду в складі інтегрованоїсистеми безпеки повинна забезпечувати виконання наступних функцій [4]: пряме відеоспостереження оператором контрольованої зони, виявлення та ідентифікацію суб'єктів спостереження – людей, транспортних засобів, майна, елементів об'єктової інфраструктури; передачу візуальної інформації про стан охоронюваних зон, приміщень, периметра і території об'єкта в пункт охорони для відеоверіфікаціі тривог – підтвердження за допомогою відеоспостереження факту порушення зон охорони та виявлення помилкових спрацьовувань охоронної сигналізації; запис відеоінформації в архів для подальшого аналізу стану об'єкту, що охороняється (зони), тривожних ситуацій, ідентифікації порушників та інших завдань.

Розрізняють три основні можливості перегляду відеоінформації:

1. Локальне спостереження безпосередньо з виходу пристроїв відеозапису або сервера – застосовується для моніторингу території невеликих об'єктів (в роздрібній торгівлі, банках і на підприємствах малого бізнесу).

2. Віддалене спостереження за допомогою ПК – для перегляду прямого або записаного відеозображення використовується ПК з встановленим спеціальним додатком до клієнтського ПЗ або веб-браузером.

3. Мобільний спостереження дозволяє охоронцеві, що знаходиться на території об'єкта, миттєво перевірити, що відображає відеоспостереження.

Мобільний спостереження має великий потенціал в плані забезпечення оперативної і злагодженої роботи груп швидкого реагування та мобільного охорони.

Автоматичний запис відеоінформації в архів може проводитися безперервно, періодично за розкладом, по спрацьовуванню сенсорів, по спрацьовуванню відеодетектора відеонагляду.

Технічні засоби архівації повинні забезпечувати зберігання необхідних обсягів відеоінформації протягом часу, який задається умовами і режимом охорони об'єкта. рекомендований час зберігання архіву не менше 15 діб.

Типовий склад системи відеонагляду (рис. 2.15) містить відеокамери, кількість яких визначається завданнями, покладеними на відеосистему, каналів передачі відеосигналу від кожної відеокамери до пристроїв обробки та зберігання і відеомоніторів як пристроїв відображення відеоінформації [8].

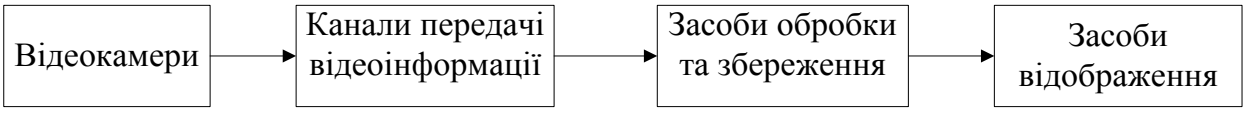


Рисунок 2.15 – Узагальнена структурна схема відеонагляду

Основні апаратно-технічні та програмні засоби системи відеонагляду по функціональним призначенням поділяють на [12]: джерела відеосигналу (відеокамери з об'єктивами); пристрої аналого-цифрового перетворення відеосигналу; пристрої комутації і передачі відеосигналу; пристрої відеозапису, цифрові відеореєстратори; пристрої виведення відеозображення (відеомонітори); пристрої прийому і обробки відеоданих.

Додатково до складу відеонагляду повинні входити: блоки живлення, комутаційне обладнання, апаратура передачі відеосигналу по різних каналах, пристрої кріплення і повороту відеокамер, кожухи для відеокамер, засоби освітлення та інфрачервоного підсвічування і інше.

Один з можливих варіантів побудови відеонагляду представлений на рис. 2.16.

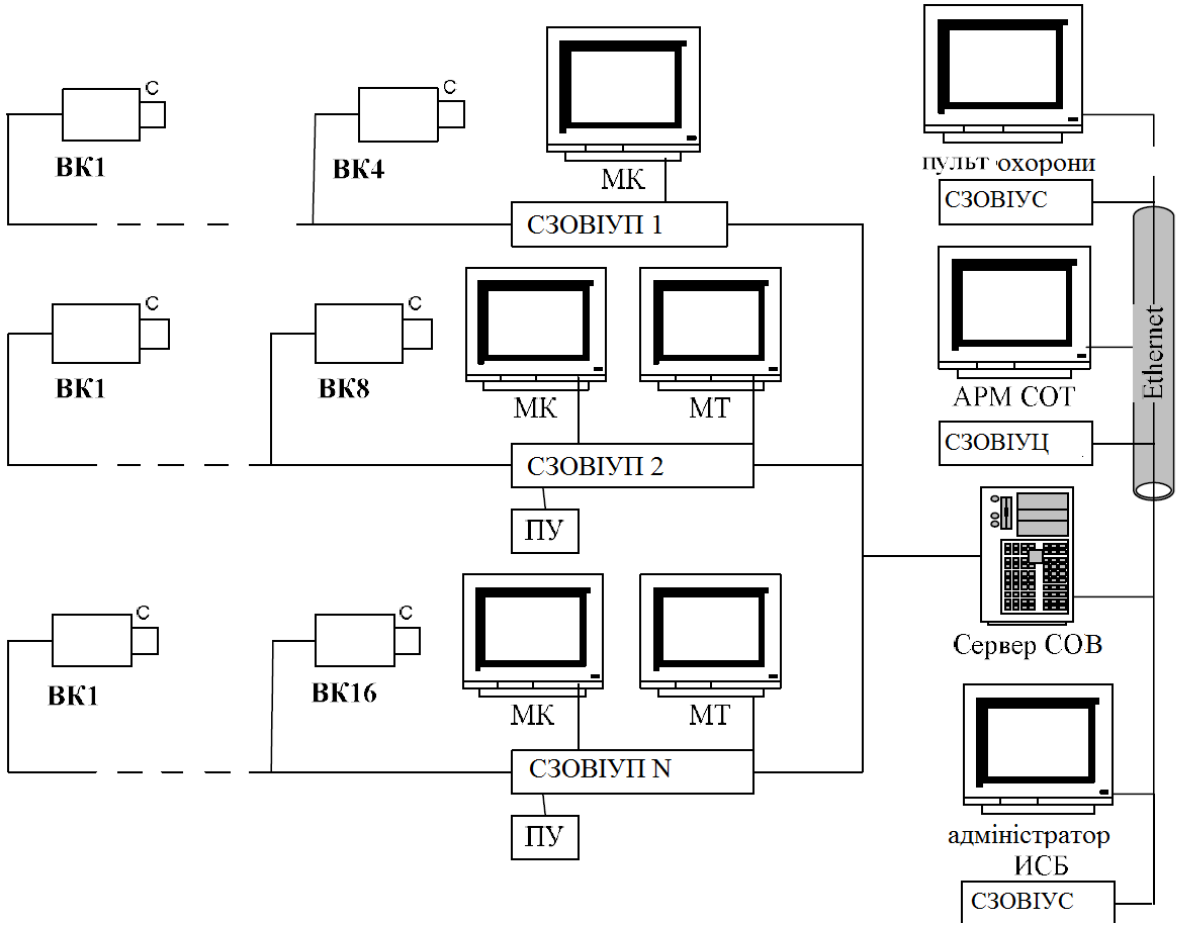


Рисунок 2.16 – Структурна схема системи охоронного відеонагляду

СЗОВІУЦ – система збору, обробки відеоінформації та управління центральна; СЗОВІУС – система збору, обробки відеоінформації та управління станційна; СЗОВІУП 1... N – система збору, обробки відеоінформації та управління периферійна; АРМ – автоматизоване робоче місце; ПУ – пульт управління; МК – монітор контролю; МТ – монітор тривоги; ВК – відеокамера

2.8.2 Джерела відеосигналу (відеокамери)

Відеокамера являє собою оптико-електронний пристрій, яке перетворює оптичне зображення об'єкта, що спостерігається в електричний відеосигнал певного стандарту (набору вимог до структурою і характером складових відеосигналу, що дозволяє стандартизувати процес прийому/передачі відеозображень) [2, 4. 7, 8].

2.8.3 Поворотні відеокамери

Поворотна відеокамера – конструктивно закінчений вузол, що складається з відеокамери, об'єктива з трансфокатором, поворотного пристрою, блоку живлення, приймача сигналів телеуправління і кожуха.

Дистанційне керування об'єктивом і поворотним пристроєм дозволяє орієнтувати відеокамеру як по азимуту, так і за кутом огляду [8].

Управління аналогової PTZ-камери проводиться з використанням інтерфейсу RS-485 і спеціального протоколу.

Найбільш поширеними є протоколи Pelco-P , Pelco-D. Камера підключається до спеціалізованого пульту управління. він дозволяє управляти поворотним пристроєм по двох координатах, фокусною відстанню об'єктива, а також швидкістю повороту. один пульт підтримує управління до 256 камер.

Основні функції і можливості PTZ -камери:

– поворот в горизонтальній площині на 360 ° і на 180 ° в вертикальній площині;

– x12... x36-кратне оптичне і x10... x25-кратне цифрове збільшення;

– 4... 256 точок предустановки - точок спостереження відеокамери з заздалегідь встановленими під час налаштування параметрами кутів у вертикальній і горизонтальній площинах і фокусом об'єктива;

– 1... 32 маршрути автопатрулирования – послідовного перегляду відеокамерою декількох точок предустановки;

– автоматичне сканування заданого сектора спостереження;

– тривожні входи, службовці для підключення зовнішнього обладнання (при подачі сигналу на тривожний вхід відеокамера повертається в заздалегідь задану точку попередньо встановлені);

– "авто стеження" - режим, при якому відеокамера автоматично "Захоплює" найбільший об'єкт в кадрі, слід за ним на 360° ПЗ горизонталі і 90° ПЗ вертикалі. Відеокамера автоматично наближає рухомий об'єкт, зберігаючи його в центрі кадру.

Плюс PTZ-відеокамери полягає в тому, що вона дозволяє контролювати великі території.

2.8.4 Інфрачервоне підсвічування

Одним із способів забезпечити працездатність відеокамери в умовах недостатньої освітленості на об'єкті є організація чергового освітлення. Найпростішим і доступним є звичайне освітлення, яке при оснащенні спеціальними пристроями (реле часу, фотоелементами, охоронними сенсорами, що реагують на переміщення) може включатися і вимикатися за розкладом

2.8.5 Пристрої для запису відео (відеореєстратори)

Відеореєстратор – це пристрій, призначений для запису, відтворення і зберігання відеоінформації в складі систем відеонагляду [2, 4].

При динамічному розподілі ресурсів відеореєстратора для кожної з відеокамер існує можливість індивідуально налаштувати параметри запису (дозвіл, ступінь компресії і швидкість).

Основні параметри відеореєстраторів.

Відеоканал – сукупність технічних засобів відеонагляду, забезпечують передачу телевізійного зображення від однієї відеокамери до екрану відеомонітора в складі відеонагляду [7]. Кількість відеоканалів DVR вказує максимальну кількість відеокамер, яке допускається підключити до DVR. В основному застосовуються відеореєстратори на 4, 8, 16 відеоканалів, і рідко на 24 і 32 відеоканалу.

Видеовиходи служать для підключення пристроїв відображення відеоінформації – відеомоніторів. S-VIDEO, VGA, DVI, HDMI відеовиходи.

Найбільш затребуваними є відеовиходи – BNC і VGA.

Аудіовходи служать для підключення мікрофонів і дозволяють здійснювати синхронну аудіозапис.

Тривожні входи і виходи використовуються для підключення охоронних сенсорів і виконавчих пристроїв (сирен).

Роздільна здатність відеореєстратора вказується в пікселах ПЗ горизонталі і вертикалі. Для DVR найчастіше використовуються наступні дозволи: 352×288, 704x288, 704x576 пікселів.

Швидкість запису вказує то кількість кадрів, яке може обробити реєстратор за 1 секунду. При вказівці швидкості на систему потрібно враховувати кількість відеоканалів конкретного відеореєстратора. так для 4-х канального DVR швидкість запису може становити 25, 50, 100 кадрів в секунду, для 16 канального реєстратора – 100, 200, 400 кадрів в секунду на систему.

2.8.6 Передача відеоінформації в системі відеонагляду

Необхідно передавати відеоінформацію від відеокамер до обладнанню, встановленому на постах охорони

Використовуються кілька основних способів передачі відеосигналу: по коаксіальному кабелю, по кабелю «вита пара» і по волоконно-оптичних кабелю. Коаксіальний кабель найбільш поширений у системах відеонагляду.

Це надійний і недорогий спосіб передачі, проте, він має свої недоліки. при передачі відеосигналу на відстань понад 300 м якість відеосигналу погіршується – відбувається падіння рівня сигналу, можуть виникати частотні спотворення, які призводять до зниження чіткості зображення [7].

При відстані до 1,5 км використовують технології та устаткування передачі відеосигналу по кабелю типу «кручена пара». При цьому не потрібно встановлювати підсилювачі. Дана технологія забезпечує стійкість до перешкод, створюваним зовнішніми джерелами.

До складу системи входить спеціальний передавач, кабель кручена пара і приймач. Використання кручений пари дозволяє виробляти передачу різної інформації – відеосигналу, аудиосигнала, даних керування, телефонії та ін. При цьому кількість переданих по одному кабелю сигналів обмежується тільки числом кручених пар в кабелі. Можливість використання вже наявних ліній зв'язку знижує вартість СОВ. В цілому, прокладка кабелю «вита пара» обходиться істотно дешевше, ніж монтажні роботи з прокладання коаксіальних або волоконнооптичних ліній.

Волоконнооптичні системи передачі відеосигналу стійкі до електромагнітним і радіочастотним перешкод, забезпечують передачу відеосигналу на відстань до десятків кілометрів без використання підсилювачів і ефективні для систем відеонагляду територіально-розподілених об'єктів.

У традиційних аналогових системах відеонагляду може використовуватися бездротової спосіб передачі сигналу від камери до

монітора, використовує радіочастотну або інфрачервону передачу даних. В цифрових системах використання бездротових мереж WiFi дозволяє перенаправити дані до будь-якого віддаленого користувача. Такі пристрої працюють в діапазонах більш високих частот, ніж використовуються в мовному телебаченні – 920 МГц, 2,4 ГГц, 5,8 ГГц.

2.8.7 Мережеві технології

Ip камери цифрова відеонагляду – це система, в якій відеосигнал від відеокамер перетвориться в цифрову форму за допомогою аналого-цифрового перетворювача і далі обробляється в системі відеонагляду в цифровому вигляді [7].

Цифрова відеокамера, яка передає відеопотік в цифровому форматі ПЗ мережі Ethernet з використанням протоколу IP (Internet Protocol), називається IP-камери. Системи відеоспостереження на базі IP-камер часто називають системами мережного відеоспостереження або IP-відеоспостереження.

Вони використовують дротову або бездротову IP-мережа як середовище передачі відео-, аудіопотоків і інших даних. система мережевого відеоспостереження дозволяє переглядати і записувати відеоінформацію з будь-якої точки мережі, незалежно від того, локальна це мережу або глобальна, така як Інтернет.

Активне впровадження IP-систем в охоронному телебаченні обумовлено рядом причин: відсутність спотворень зображення при передачі і зберіганні інформації в цифровому вигляді; реалізація нових функцій завдяки можливостям відеоаналізу; економічна ефективність для великих відеосистем.

Базовими компонентами системи мережевого відеоспостереження є мережеві відеокамери, відеокодери (переводять відеосигнали від аналогових камер в цифрові IP -відеопотокі) і ПЗ для управління відео.

Інші компоненти, включаючи мережу, системи зберігання та сервери являє собою стандартне IT-обладнання.

Будучи мережевим пристроєм, кожна IP -камера в мережі має свій IP - адреса. IP-камери можуть передавати відеоінформацію як в стислому, так і в стислому вигляді за допомогою покадрових (MJPG) і потокових (MPEG-4, H.264) методів. Як протоколів транспортного рівня в IP-камери можуть використовуватися протоколи: TCP (Transmission Control Protocol – протокол управління передачею), UDP (User Datagram Protocol – протокол призначених для користувача датаграм), RTP (Real-time Transport Protocol – використовується при передачі трафіку реального часу) та інші транспортні протоколи мережевого протоколу IP.

Стандартна чіткість для мережевих камер: 640x480 точок. Існують відеокамери з мегапіксельними дозволами: 1280x1024, 1600x1200 і більш високими значеннями.

В системі мережевого відеоспостереження домогтися високої якості зображення простіше, ніж в аналоговій системі.

Переваги мережевих відеокамер в порівнянні з аналоговими:

– можливість побудови масштабованих розподілених систем відеоспостереження;

– широкий діапазон параметрів налаштувань роботи відеокамери;

– відсутність «прив'язки» до аналогових відеостандарті, в результаті чого можливе впровадження IP-камер зі значно вищим дозволом;

– віддалений доступ – IP-камери можна налаштовувати віддалено, забезпечивши можливість кільком авторизованим користувачам переглядати зображення в режимі реального часу і записувати відео практично з будь-якої, що має доступ в мережу, точки світу;

– можливість передачі аудиопотока по мережі паралельно з відеопотоком;

– можливість передачі потоку з високим стисненням, яке дозволяє економити місце на цифрових носіях, не вимагаючи при цьому високопродуктивного відеореєстратора.

Недоліки мережевих відеокамер в порівнянні з аналоговими:

– ціна на IP-камери вище, ніж у аналогових камер, але якщо розглядати обладнання об'єкта системою відеоспостереження в цілому, то ціни на "проект + обладнання + монтаж" є порівнянними;

– чутливість матриці мегапіксельних IP-камер як правило істотно нижче, ніж у аналогових камер;

– необхідність наявності значної обчислювальної потужності пристрою обробки інформації для декомпресії відеопотоку на комп'ютерної платформі (клієнта), що збільшує витрати;

– схильність до зовнішнього мережевого впливу (злому);

– апаратне зависання (при відсутності функції Watchdog timer – таймер перезавантаження).

2.9 Висновки

Питання забезпечення ефективного захисту об'єктів, розглянуті вище, сприяють формуванню базової теоретичної і практичної підготовки в області інтегрованих комплексних систем безпеки. Вивчення основних термінів, визначень і принципів організації інтегрованих комплексних систем безпеки дозволяє вирішувати наступні завдання проектування і аналізу функціонування комплексних систем безпеки: вибір варіанту охорони об'єкту з використанням комплексу технічних засобів забезпечення безпеки відповідно до вимог технічної укріпленості об'єкта; виконання основних етапів проектування комплексних систем безпеки з використанням основних принципів розробленої концепції безпеки; розробка структурної схеми інтегрованої комплексної системи безпеки на основі даних про вхідні в неї підсистеми контролю доступу, охоронно-пожежної сигналізації та систем

відеонагляду безпеки; синтез окремих компонентів комплексних систем безпеки на базі готових уніфікованих функціональних вузлів, розрахунок їх основних параметрів і характеристик; виконання оптимізації структури комплексної системи безпеки з використанням методів оцінки ефективності її функціонування.

Виконання зазначених завдань розвиває здатності збирати, обробляти, аналізувати і систематизувати науково-технічну інформацію по темі дослідження інтегрованих комплексних систем безпеки, вибирати перспективні методи вирішення професійних завдань на основі сучасного розвитку оптико-електронних і телевізійних систем безпеки.

3 РОЗРОБКА МОДЕЛІ ІНТЕГРОВАНОЇ КОМПЛЕКСНОЇ СИСТЕМИ БЕЗПЕКИ СПЕЦІАЛЬНОГО ОБ'ЄКТУ

Розроблена модель інтегровананої комплексної системи безпеки спеціального об'єкту для декількох банківських приміщень: офіс "open space" для якого спроектовано систему охоронної, тривожної, пожежної сигналізації та система контролю і управління доступом; банківське сховище для якого створено проект системи відеонагляду.

Для системи охоронної, тривожної, пожежної сигналізації та системи контролю і управління доступом обрано технічні засоби інтегрованих комплексних систем безпеки науково виробничого об'єднання "Болід".

Так само система відеонагляду створена на базі технічних засобів "Болід". Це дає змогу керувати та налагоджувати відонагляд з центрального пульту керування усією системою.

Інженерні та програмні рішення цих виробників відповідають усім нормам та вимогам проектування високозахищених інтегрованих комплексних систем безпеки.

3.1 Модель охоронно-пожежної системи

Система охоронної, тривожної та пожежної сигналізації "Болід" у своїх рішеннях має такі переваги перед конкуруючими фірмами:

– комбіновані охороно-пожежні сенсори з вбудованим сигнально-звуковим засобом підняття тривоги;

– безперервне опитування сенсорів кожні 38 сек;

– високозахищений канал зв'язку, інформація передається в окремовиділеній кабельній мережі по інтерфейсу RS-485 та RS-232;

– висока завадостійкість;

– кількість сенсорів підключених до одного контролера 120;

– зручний інтерфейс ПЗ для центрального пульту керування, регулярні оновлення і цілодобова підтримка;

– зв’язок на фізичному рівні забезпечується двопровідною лінією надстійкою до вогню (рис. 3.1).

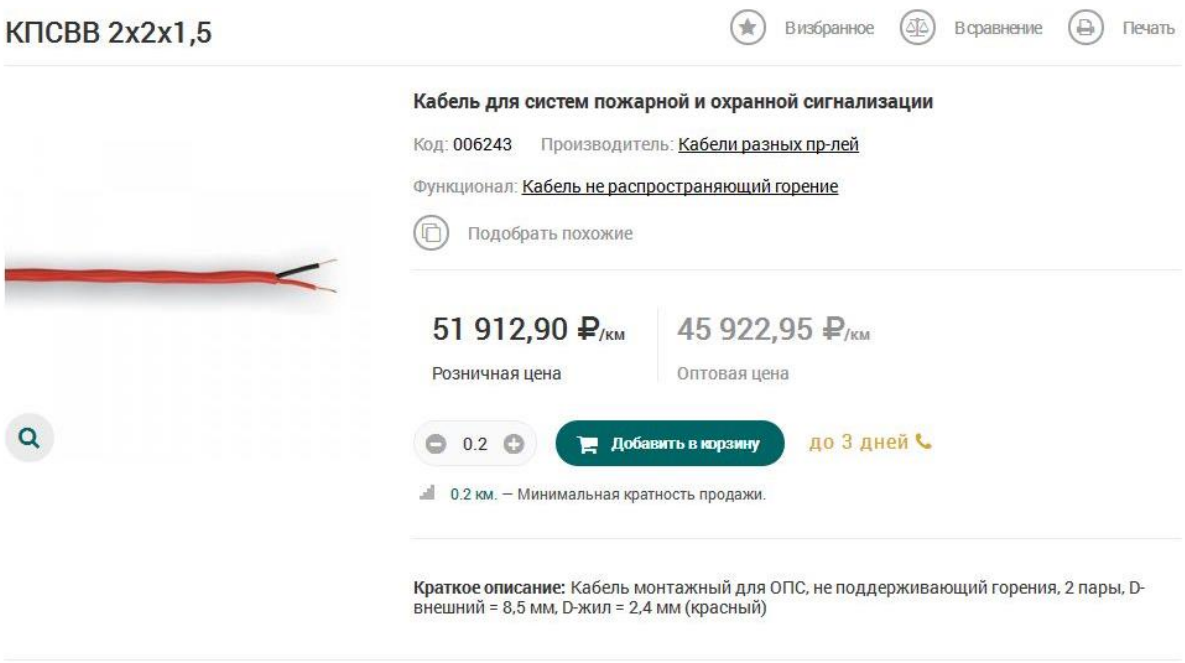


Рисунок 3.1 – Двопровідний кабель надстійкий до вогню

Сенсор охороно-пожежний з сповіщувачем, чутливий елемент оптико-електронний ІЧ, що також виявляє задимлення (рис. 3.2).

Рисунок 3.2 – Вигляд моделі адресного аналогового охороно-пожежного ІЧ сенсора з сповіщувачем

Основні характеристики:

- дальність дії 20-80 м;
- кут огляду 90°;
- напруга живлення 7-11 в;
- струм живлення 1,7 мА;
- захист корпусу ip40;
- термін придатності 10 років;
- інтерфейси: RS-485;
- завадостійкість 7 рівня;
- можливість програмувати сенсор.

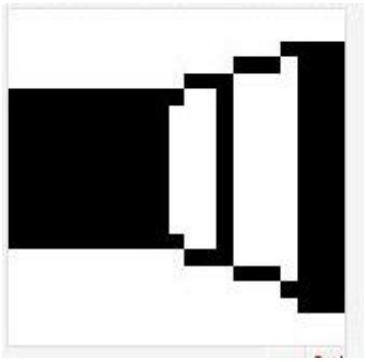


Рисунок 3.3 – Умовне зображення на схемі адресного аналогового охороно-пожежного ІЧ сенсора з сповіщувачем

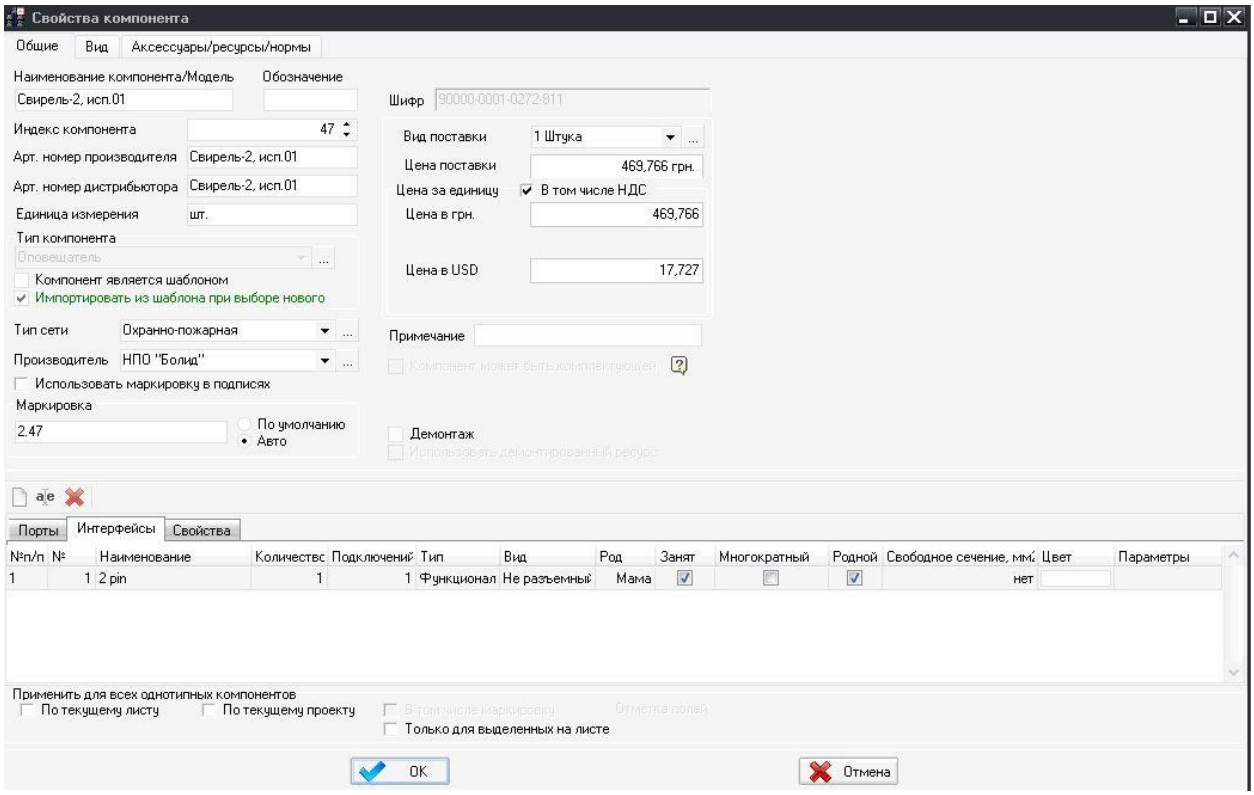


Рисунок 3.4 – Інформаційне меню з даними адресного аналогового охороно-пожежного ІЧ сенсора з сповіщувачем у СКС-Експерт

Контролер двопровідної ліній зв’язку (рис. 3.5)

Рисунок 3.5 – Модель контролера двопровідної ліній зв’язку

Основні характеристики:

– довжина лінії 600м;
– підтримує 120 сенсорів;
– виконує опитування кожні 38 секунд;

– порти інтерфейсів: RS-485, RS-232;
– напруга живлення 10-30 В;
– струм живлення 160 мА;
– захист корпусу ip40;
– термін придатності 10 років;
– завадостійкість 7 рівня;
– можливість програмувати контролер.

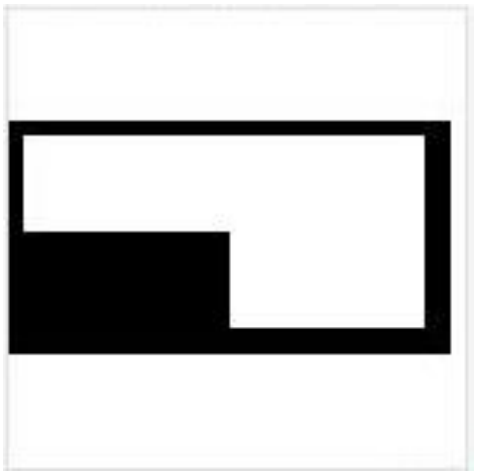


Рисунок 3.6 – Умовне зображення на схемі контролера двопровідної ліній зв’язку

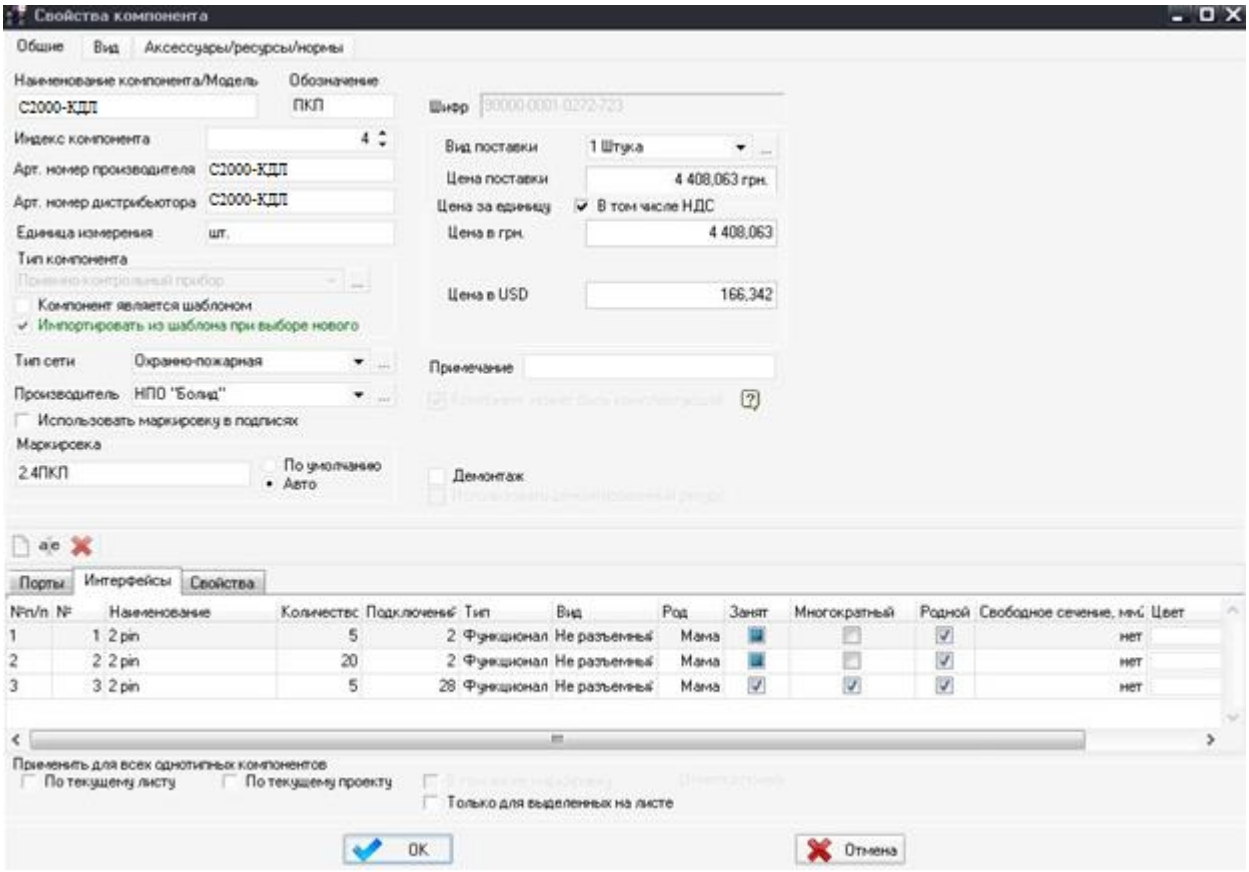


Рисунок 3.7 – Інформаційне меню з даними у СКС-Експерт контролера двопровідної ліній зв’язку

Пульт централізованої охорони (рис. 3.8)

Являється робочою станцією/сервером для управління та контролю системою охоронної, тривожної та пожежної сигналізації “Болід” а також СКУД з можливістю сповіщення охорони, керівництва та поліції про проникнення.

Основні характеристики:

– Процесор Intel Core i5, з частотою 2,5 ГГц;

– 8 Гб Оперативної пам’яті;

– Канали з’язку: телефонна лфнія, GSM модуль, Ethernet, інтерфейсна шина RS-485, RS-232.

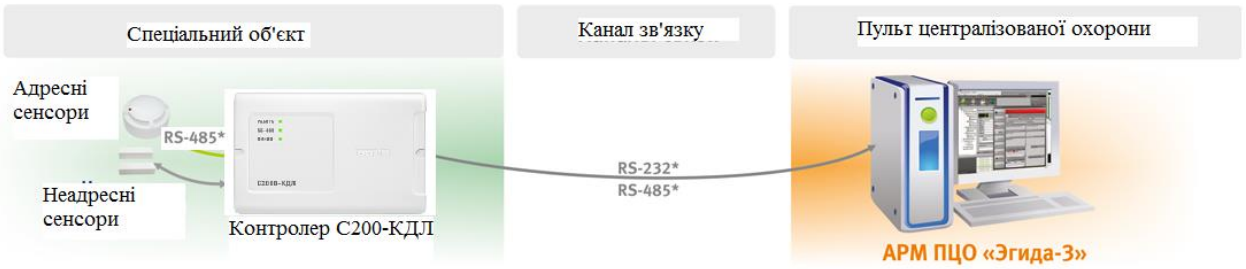


Рисунок 3.8 – Умовна схема підключення пульту централізованої охорони до охоронно-пожежної системи

Розробка проекту виконана в професійному ПЗ СКС-Експерт задля більш точного та якісного схематичного вигляду професійного рівня (рис. 3.9, 3.10)

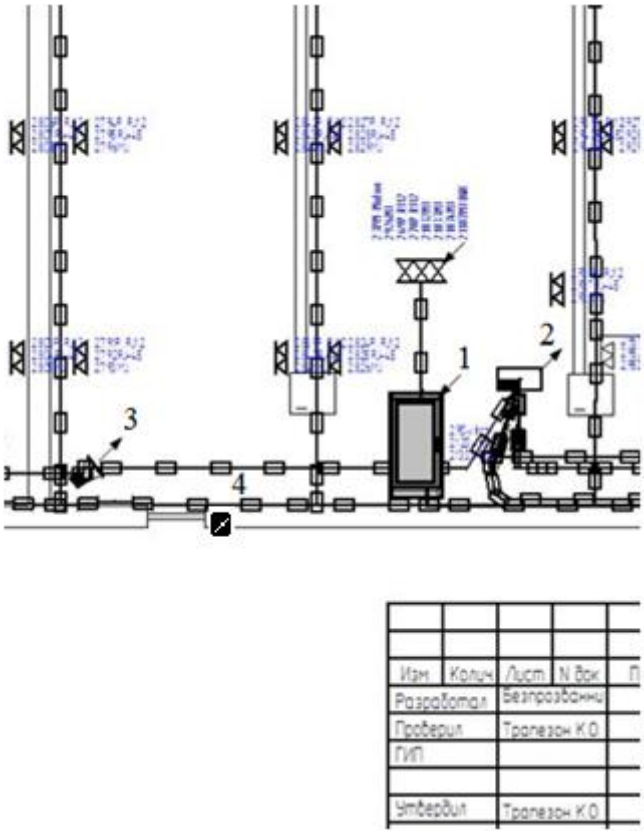


Рисунок 3.9 – Частина структурної схеми інтегрованої комплексної системи безпеки спеціального об’єкту система охоронної, тривожної та пожежної сигналізації “Болід” та СКУД. Зображено: 1) пульт централізованої охорони, доповнене ДБЖ; 2) контролер; 3) сенсор; 4) сенсор СКУД

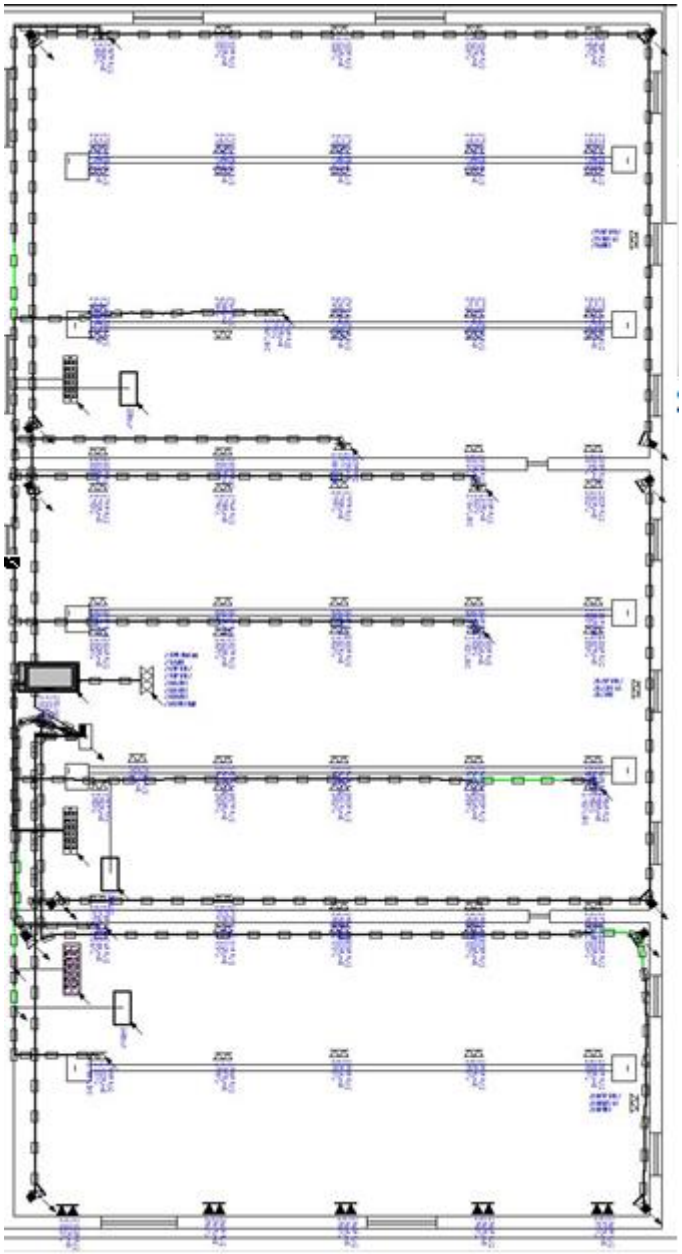


Рисунок 3.10 – Схема структурна інтегровананої комплексної системи безпеки спеціального об’єкту система охоронної, тривожної та пожежної сигналізації “Болід” та СКУД

СКУД (рис. 3.11)

Proxy ЗМА зчитувач

Основні характеристики:

– інтерфейс RS-232;

– напруга живлення 8-15 В;

– струм живлення 160 мА;
– захист корпусу ip40;
– термін придатності 10 років;
– завадостійкість 7 рівня;
– можливість програмувати контролер.

Сенсор магнітно-контактний

Основні характеристики:

– інтерфейс RS-232;
– струм живлення 0,5 мА;
– захист корпусу ip40;
– термін придатності 10 років.

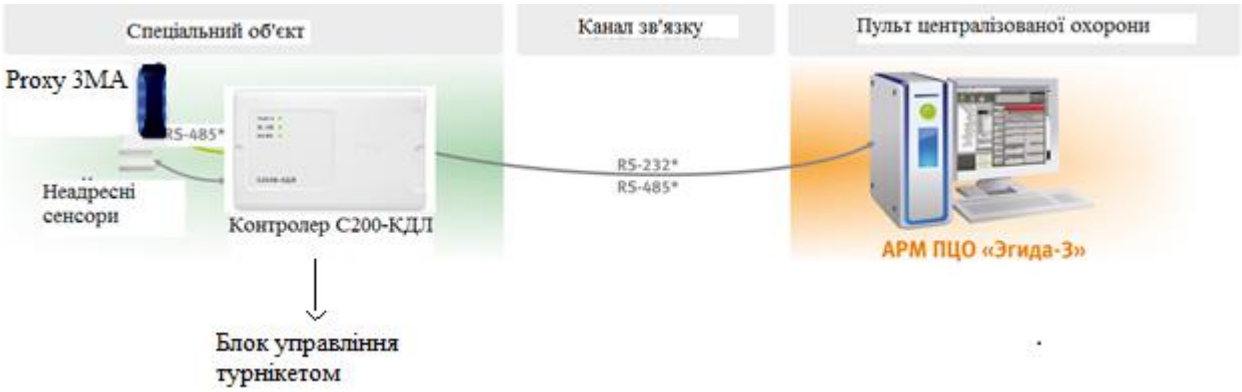


Рисунок 3.11 – Умовна схема підключення пульту централізованої охорони до СКУД

Зручний інтерфейс пульта централізованої охорони базується на ОС Windows 7 (рис. 3.12, 3.13).

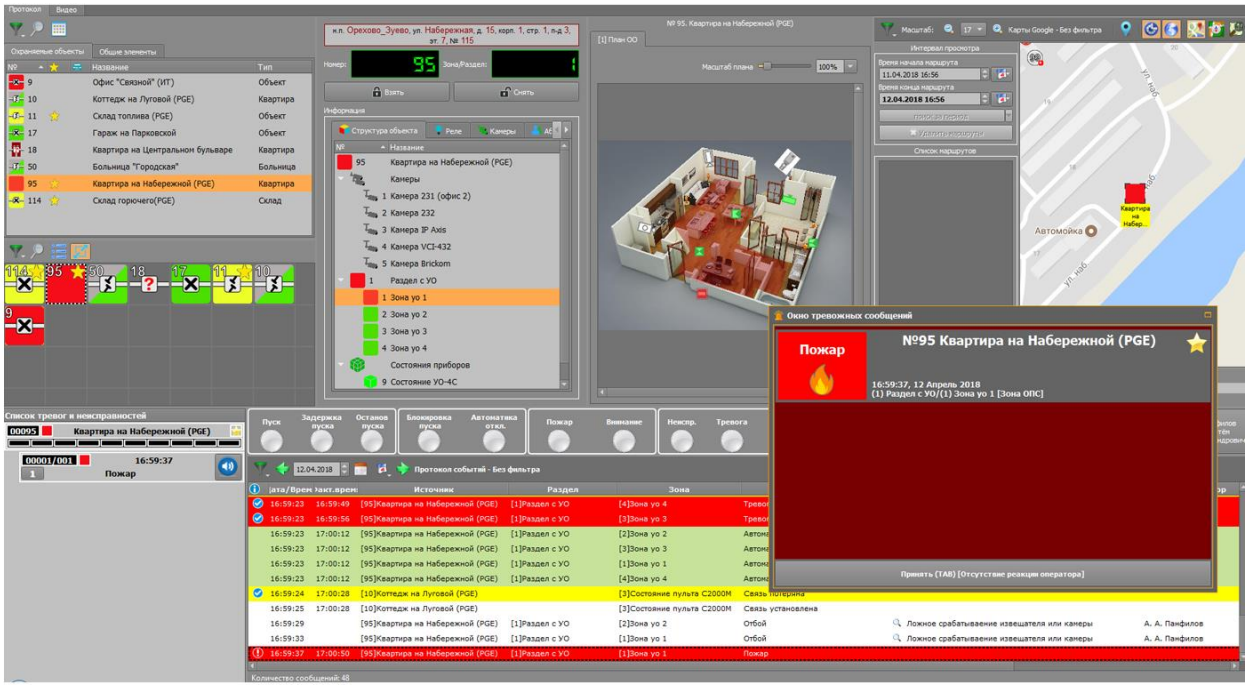


Рисунок 3.12 – Приклад №1 зображення інтерфейсу інтегрованої комплексної системи безпеки спеціального об’єкту на базі систем “Болід”

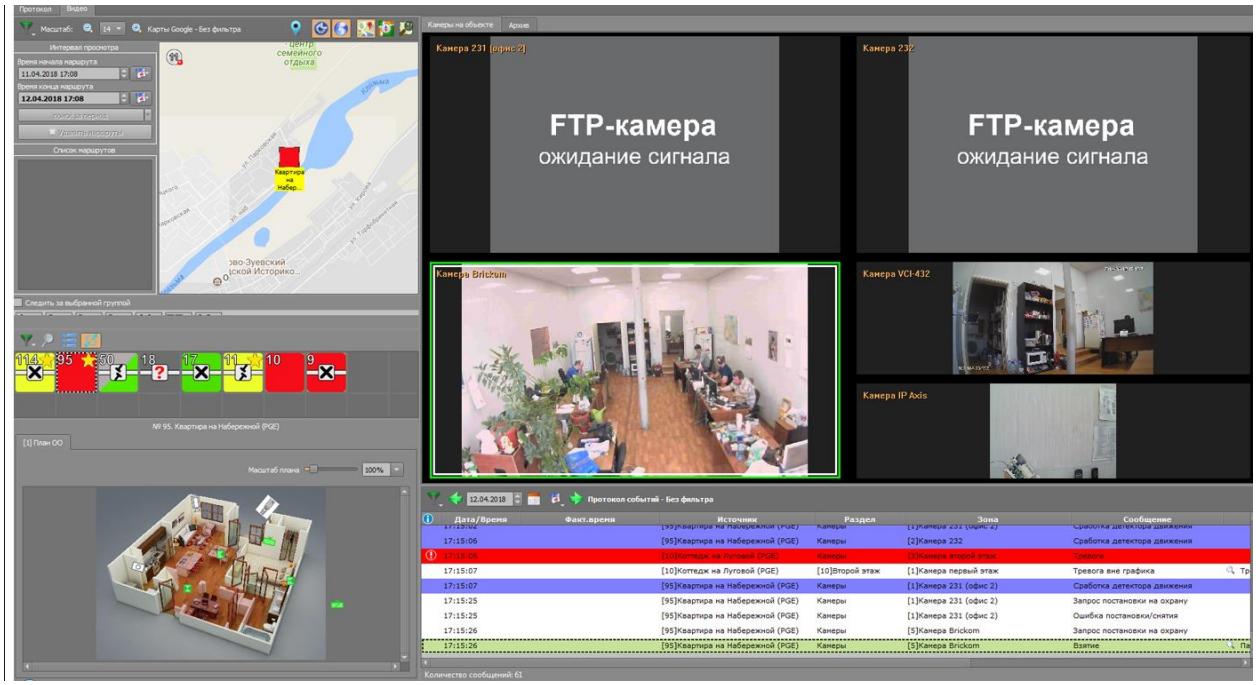


Рисунок 3.13 – Приклад №2 зображення інтерфейсу інтегрованої комплексної системи безпеки спеціального об’єкту на базі систем “Болід”

3.2 Модель системи відеонагляду

Система відеонагляду інтегрованої комплексної системи безпеки спеціального об’єкту спроектована також в СКС-Експерт для вищої схематичної точності та в IP Video System Design Tool 7 для наглядності якості обраних камер. На рис. 3.14 зображена кімната контролю з розташованими в ній робочого місця оператора та відеореєстратор.

Переваги систем відеонагляду “Болід”:

– можливість інтергації з іншими системами цього виробника, що зпрощує встановлення та керування цілісною системою охорони;

– здійснює отримання і запис відео в форматах MJPEG, MPEG-4, H.264 безпосередньо в контейнери AVI. Також можливе отримання і запис звуку в кодеках PCM, G.711, G.726, AAC;

– ПЗ виробницьва “Болід” дає змогу не лише вести нагляд, а й ідентифікувати людей та події.

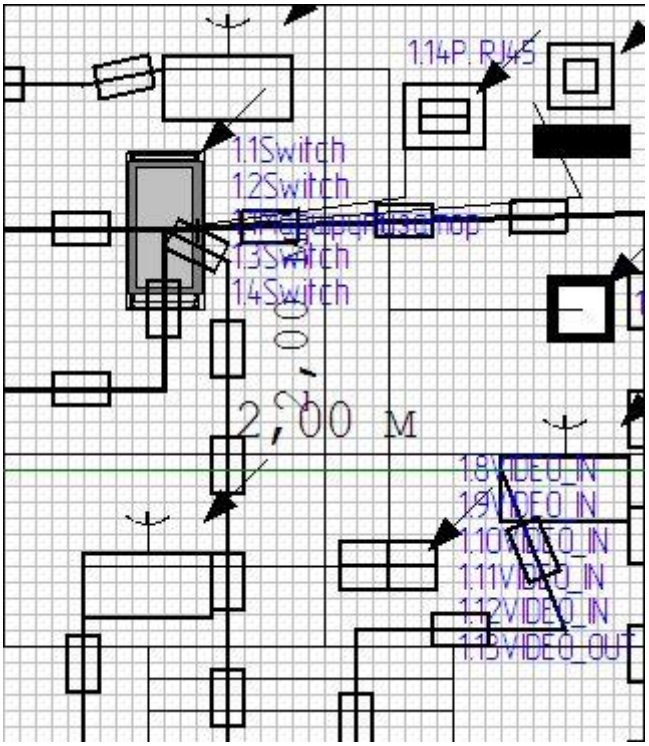


Рисунок 3.14 – Кімната контролю за системою відеонагляду

На рис. 3.15 зображена кімната в якій ведеться відеонагляд за умовним сейфом. Менша камера є аналоговою, відеосигнал з неї перетворюється йде по коаксіальній лінії до балуна (перетворювача), а далі по “витій парі” надходить до відеореєстратора. Дві більші камери є IP-камерами від них сигнал одразу по витій парі надходить до відеореєстратора.

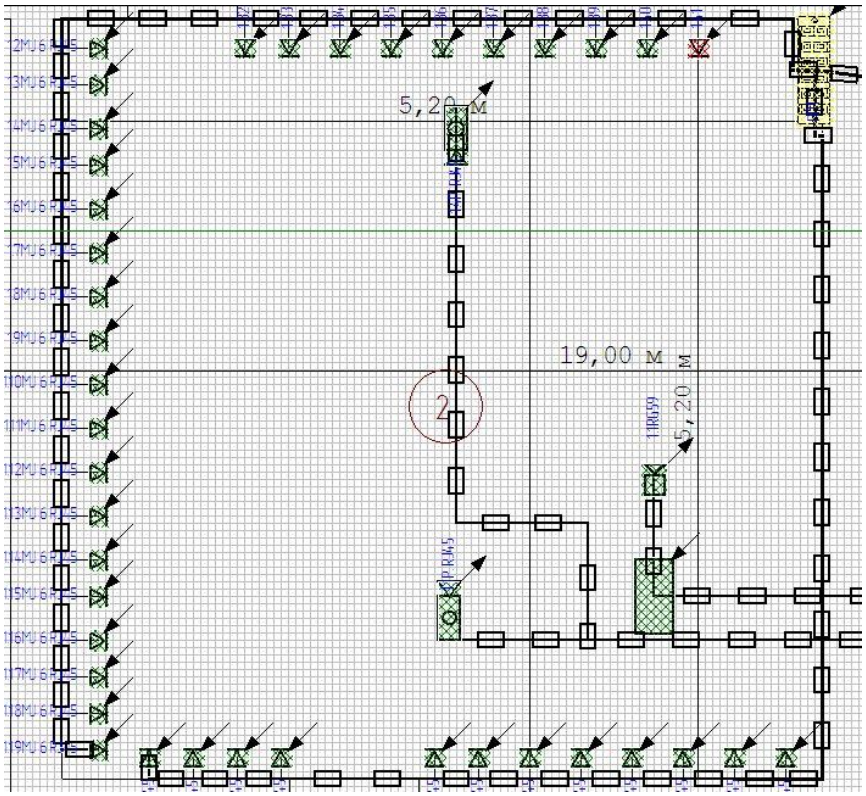


Рисунок 3.15 – Кімната відеонагляду

На рис. 3.16, 3.17, 3.18 інформативне меню стану та підключення відеокамер та балуна відповідно СКС-Експерт.

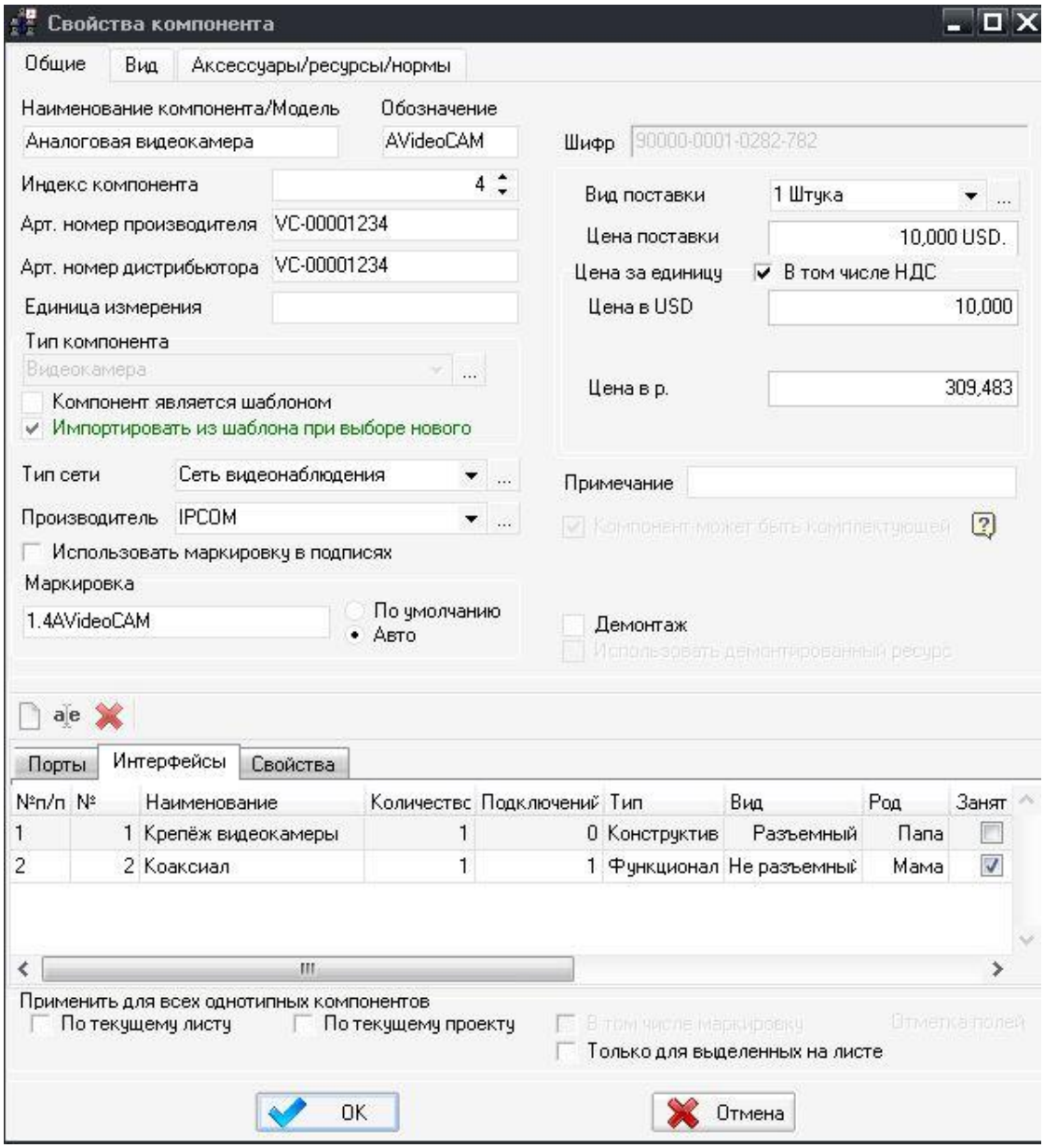


Рисунок 3.16 – Інформативне меню стану та підключення відеокамери аналогової

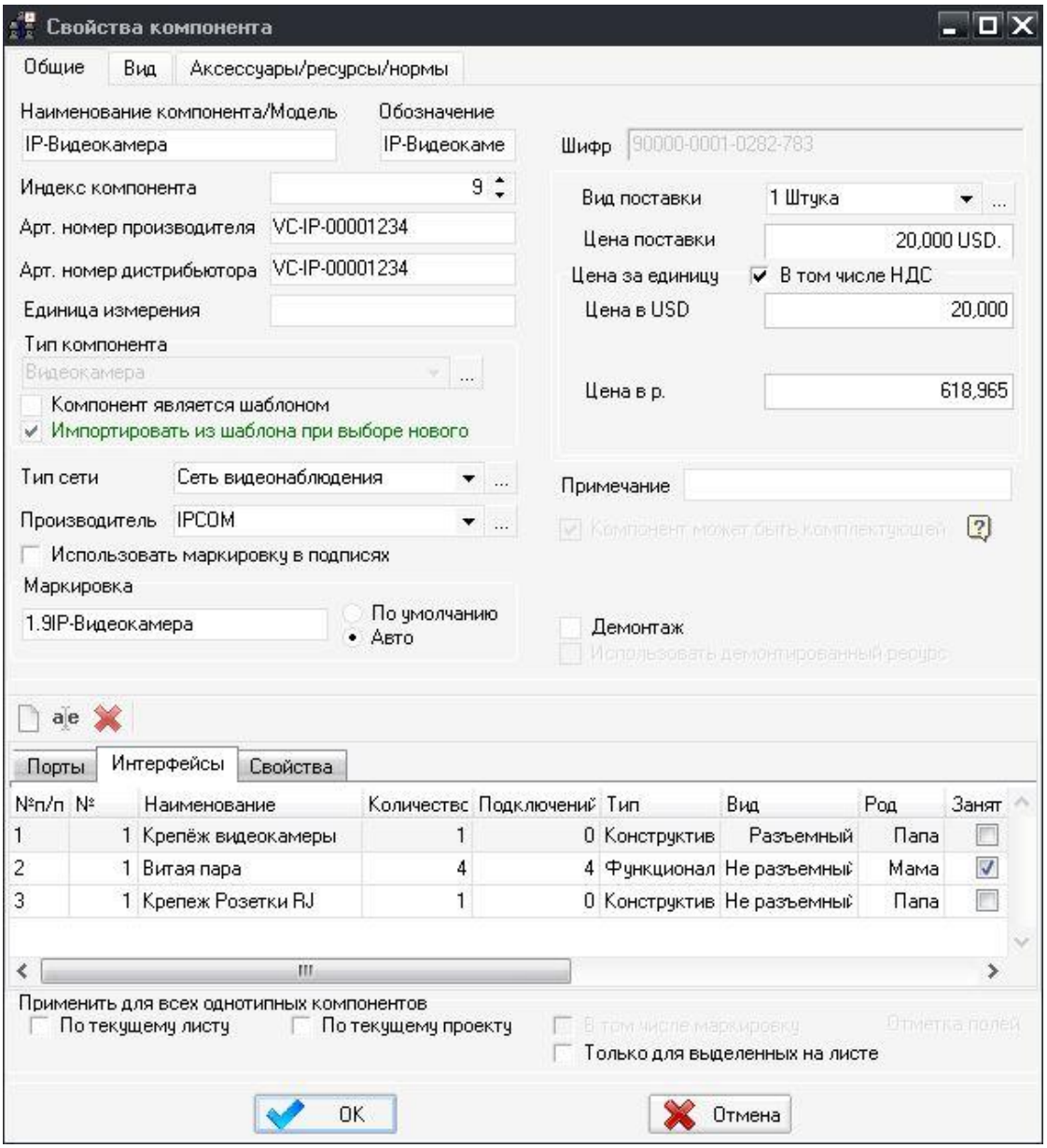


Рисунок 3.17 – Інформативне меню стану та підключення IP-відеокамери

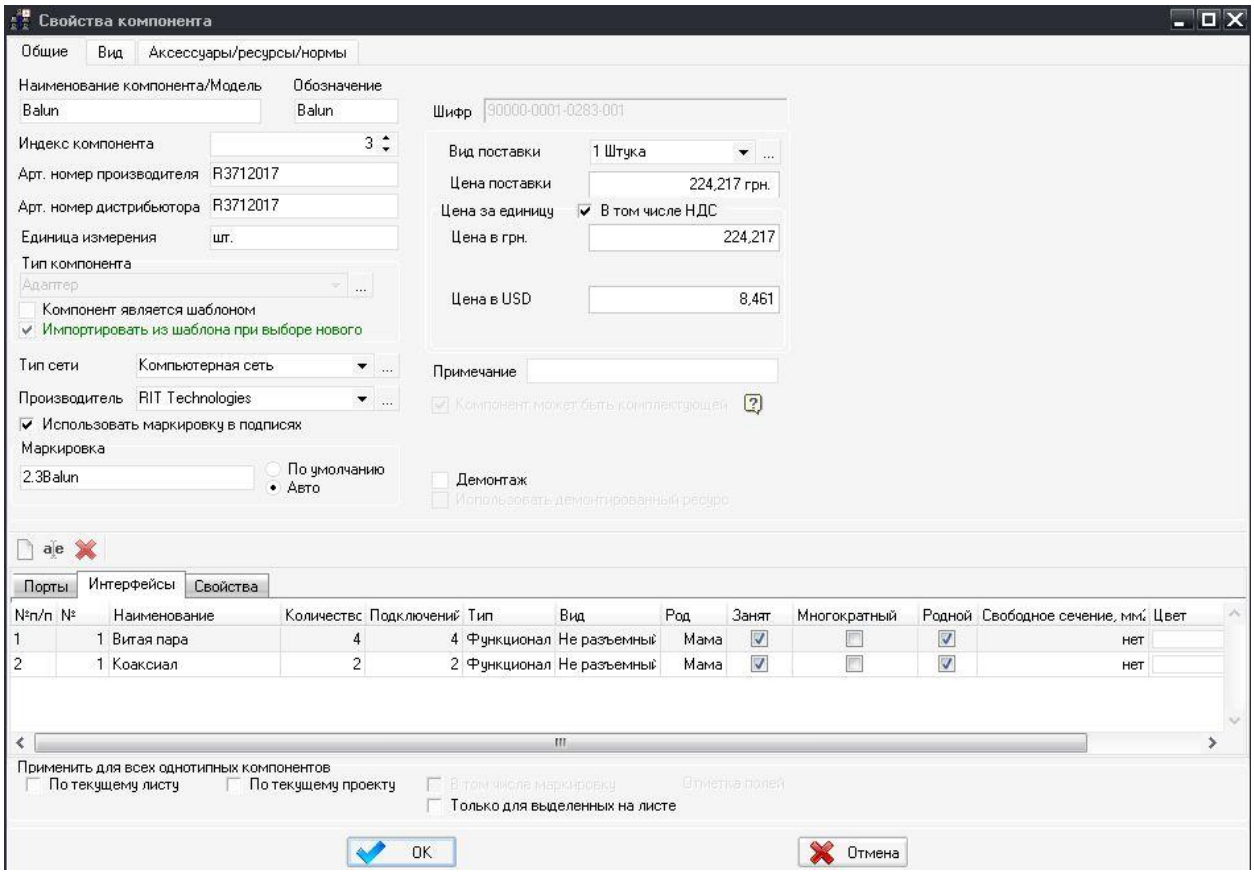


Рисунок 3.18 – Інформативне меню стану та підключення балуна

Технічні засоби які використані для створення спроектованої системи відеонагляду: відеореєстратор RGI-0812P08 (рис. 3.19), камера аналогова (3.20) та IP (рис. 3.21), балун (рис. 3.22).

Рисунок 3.19 – Вигляд моделі відеореєстратора RGI-0812P08

Основні характеристики відеореєстратора RGI-0812P08:

– процесор вбудований двоядерний;

– ОС Linux;

– кількість потоків записи 8 каналів;

– відеовиходи: 1 hdmi, 1 vga;

– якість зображення по hdmi: 3840×2160, 1920×1080, 1280×1024, 1280×720;

– якість зображення по vga: 1920×1080, 1280×1024, 1280×720;

– багатовіконний режим 1/4/8/9;

– запис відео;

– стиснення відеосигналу h.264/h.265/mjpeg;

– формат відеозображення 8mp/6mp/5mp/4mp/3mp/1080p/720p/d1;

– швидкість запису 80 мбіт/с;

– швидкість передачі даних 48 ~ 8192 кбіт/с;

– відтворення і резервне копіювання;

– види дій включення запису, ptz-управління, запуск туру, відправка відеозаписи (video push), відправка листа по електронній пошті, знімок, передача по ftp, включення звукового попередження і висновок інформації на екран;

– детекція руху зони детекції руху: 396 (22x18), втрата відеосигналу і спроба закриття об'єктиву камери;

– синхронізація;

– функція пошуку за дату/час, подію тривоги, подіям виявлення руху і точний пошук (до секунди), smart пошук;

– резервне копіювання usb-накопичувач / мережа;

– ethernet 10/100 base-t, rj-45;

– poe 8 портів (ieee802.3at / af);

– мережеві протоколи: http/https, tcp/ip, ipv4/ipv6, rtsp, udp, ntp, dhcp, dns, ip filter, ddns, ip search (support dahua ip camera, dvr, nvs and etc.), easy4ip;

– максимальна кількість користувачів 128;
– жорсткий диск 1 sata порт, не більше 6 Тб;
– напруга живлення 48 В.

Рисунок 3.20 – Вигляд моделі відеокамери аналогової

Основні характеристики відеокамери аналогової:

– розширення зображення 1936×1097 пікселів;
– частота кадрів: 1080p(1~25 к/с), 720p(1~25/50 к/с);
– формати: hdcvi, hdtvi, ahd, cvbs;
– дальність ік підсвічування 50 м;
– режими :день-ніч авто (icr)/колір/ч/б;
– компенсація фонової засвітки dwdr;
– шумоподавлення 2d;
– кут огляду H: 106º;
– мікрофон вбудований;
– напруга живлення 12 В.

Рисунок 3.20 – Вигляд моделі відеокамери IP

Основні характеристики відеокамери IP:

– розширення зображення 1280x720 пікселів;
– частота кадрів: 1080p(1~25 к/с), 720p(1~25/50 к/с);
– формати: hdcvi, hdtvi, ahd, cvbs;
– компенсація фонової засвітки blc/hlc/dwdr;
– баланс білого авто/ручн.;
– регулювання посилення авто/ручн.;
– шумоподавлення 3d;
– дальність ік підсвічування 30 м;
– день-ніч авто (icr)/колір/ч/б;
– кут огляду H: 67º;
– веб-інтерфейс перегляд і настроювання через браузер;
– протоколи: http; tcp; arp; rtsp; rtp; udp; smtp; ftp; dhcp; dns; ddns; ipv4/v6; qos; upnp; ntp;
– максимальна кількість користувачів 20;
– максимальне напруження імпульсних перешкод 2 кв;
– напруга живлення 12 В;
– мікрофон вбудований;
– прогресивна система сканування для ідентифікації.

Рисунок 3.21 – Вигляд моделі балун (перетворювач з аналогового сигналу в цифровий)

На рис. 3.22 схема розташування камер у банківському сховищі з сейфом. Рис. 3.23 доповнює схему історією позначень зон видимості камер та оскільки наша система відеонагляду входить до інтегрованої комплексної системи безпеки спеціального об’єкту то має підтримувати високу якість запису відео, що дасть змогу гарантовано ідентифікувати будь-яку людину чи подію в зоні видимості камер. Рожевим кольором виділені зони в яких буде гарантована ідентифікація, зеленим зона моніторингу (без необхіджності індентифікації особистості але з відповідно розпізнавання об’єктів та їх дій в зоні видимості. На рис. 3. 24 та 3.25 зображені параметри встановлення камер та характеристики камер у приміщенні сховища банку.

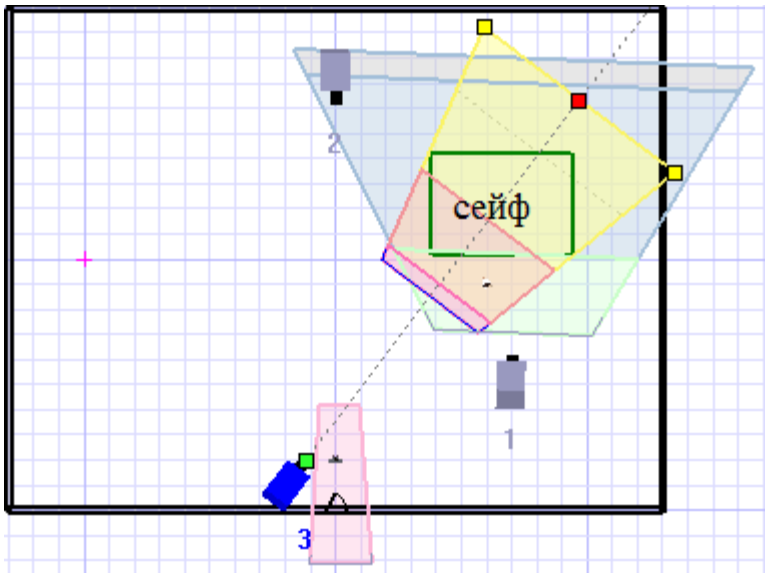


Рисунок 3.22 – Схема розташування камер у банківському сховищі з сейфом

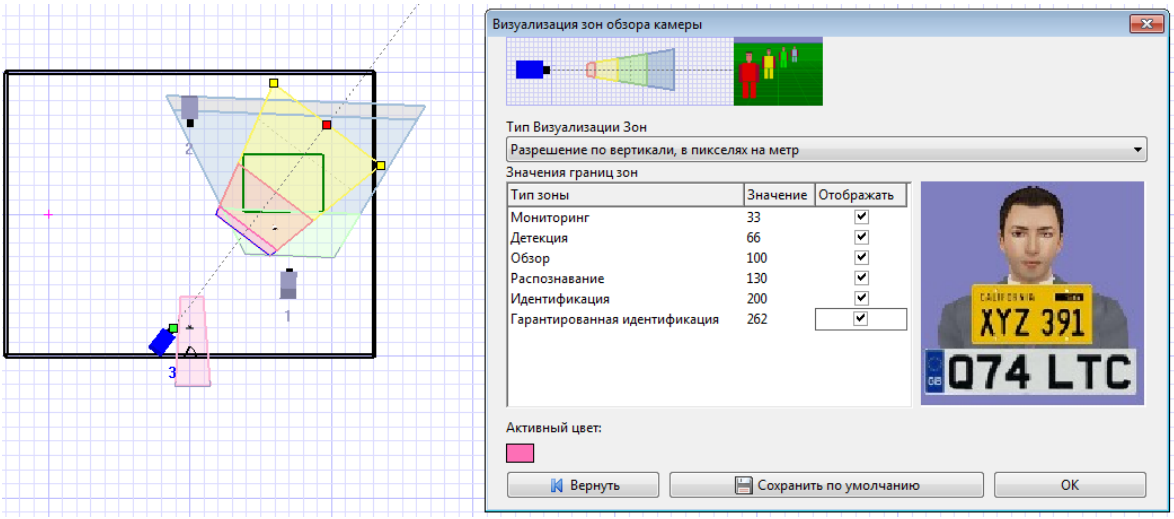


Рисунок 3.23 – Історія схеми розташування камер у банківському сховищі з розпорділенням на зони моніторингу та ідентифікації

Камера	Матрица	Выс.кам.	Рассто...	Ширин...	Высота ...	H...	Фокусн.р...	Соотн.ст...	Ниж. Гра...	X	Y	Напра...
1	1/3 "	4	12	18,3	2,8	40,4	2,6	4:3	0	17	-4	2,291831
2	1/3 "	4	12	1,6	2,6	9,5	36,4	4:3	0	10	6,2	179,3357
3	1/3 "	4	18	9,5	3,0	14,6	8,9	4:3	0	8,8	-8	37,24225

Рисунок 3.24 – Параметри встановлення камер у приміщенні сховища банку

Разрешение	Видеосжатие	Размер кадр...	FPS	Сут...	Камер	Трафик,Мб/с	Объем,Гб	Битре...	Приме...
640x480 (VGA)	MPEG4-20 (Хорошее к	7,3	30	1	1	1,79	19,4	1794	
1920x1080 (Full HD)	H.264-10 (Высокое ка	15	60	1	1	7,37	79,6	7373	
1920x1080 (Full HD)	H.264-10 (Высокое ка	15	60	1	1	7,37	79,6	7373	

Рисунок 3.25 – Характеристики камер у приміщенні сховища банку

Результат виконання програмної перевірки зон видимості камер та їх можливостей ідентифікації особистості. На рис. 3.26 відображено якість зображення з IP-камери з такими самими характеристикам як ті котрі ми використали для свого проекту. За рис. 3.23 ми побачили, що камера володіє можливістю гарантованої ідентифікації, що і продемонстровано на рис. 3.26 де ми точно бачимо обличчя людини. Також схема розташування камер зроблена наступним чином, щоб дві IP-камери контролювали вхід (рис. 3.26) та підхід до сейфу (3.28), а аналогова моніторила зону входу в сейф та його переметр (рис. 3.27). Тож якщо зловмиснику вдасться потрапити в сховище банку яке не має вікон якимось іншим чином окрім як через двері при чому, що сховище має стіни як у бомбосховища та навколо будівлі відсутні інженерні тонелі чи колодязі (залитий бетонний фундамент навколо якого втрамбований грунт з щебнем) то всеодно камери зафіксують і його, і протиправні дії.

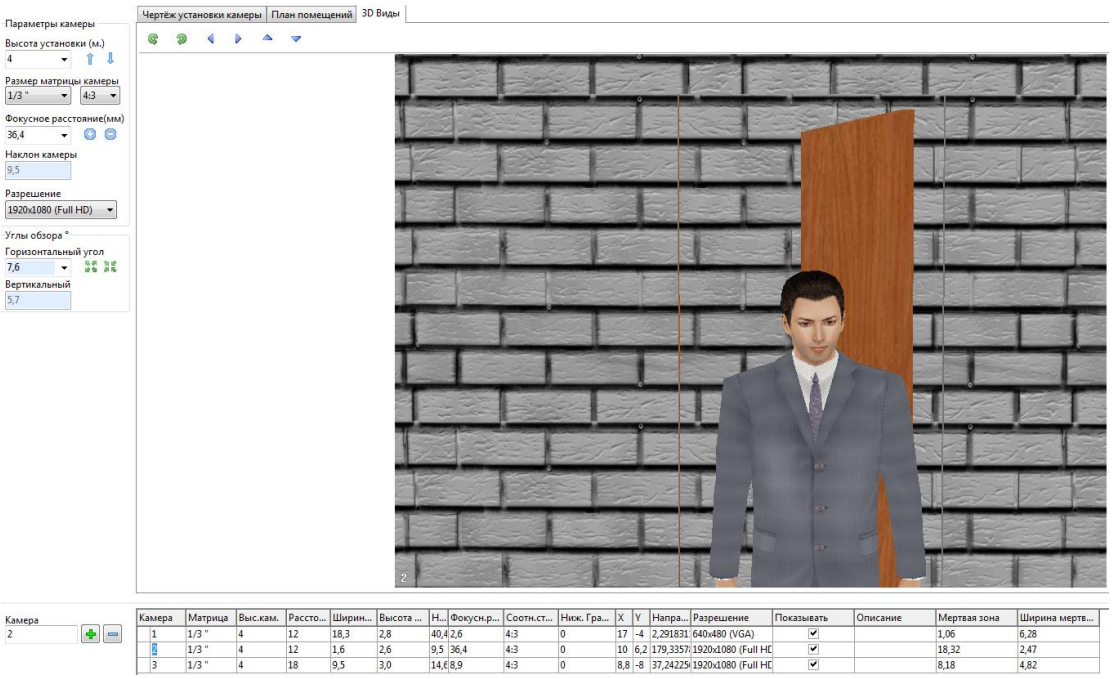


Рисунок 3.26 – Результат програмної перевірки IP-камери вона під другим номером

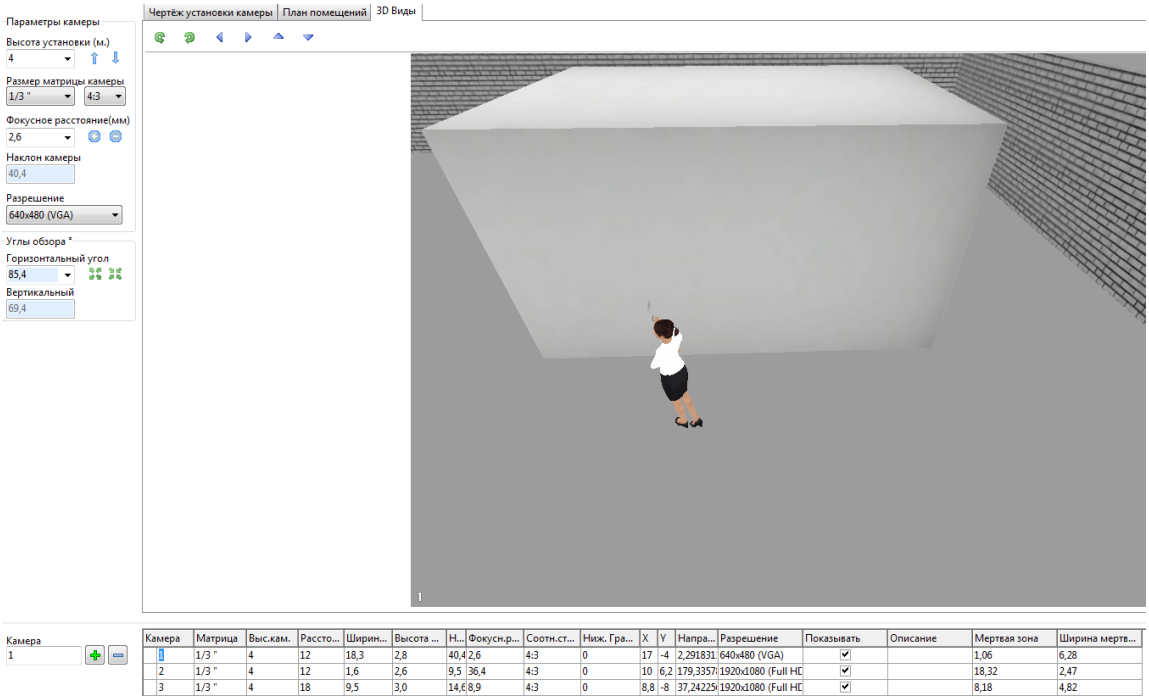


Рисунок 3.27 – Результат програмної перевірки аналогової камери, що під номером один

Рисунок 3.28 – Результат програмної перевірки IP-камери вона під третім номером

3.3 Висновки

Реалізовано проект інтегровананої комплексної системи безпеки спеціального об’єкту для декількох банківських приміщень: офіс “open space” для якого спроектовано систему охоронної, тривожної, пожежної сигналізації та система контролю і управління доступом; банківське сховище для якого створено проект системи відеонагляду.

Для системи охоронної, тривожної, пожежної сигналізації та системи контролю і управління доступом обрано технічні засоби інтегрованих комплексних систем безпеки науково виробничого об’єднання “Болід”.

Результати програмної перевірки переконливо вказують на те, що проект інтегровананої комплексної системи безпеки спеціального об’єкту виконує свої функції по захисту в повному обсязі.

4 РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ

4.1 Опис ідеї проекту

Таблиця 4.1 - Опис ідеї стартап-проекту

<table>
<tr><th>Зміст ідеї</th><th>Напрямки застосування</th><th>Вигоди для користувача</th></tr>
<tr><td rowspan="3">Описані в дисертації інженерні рішення з проектування інтегрованої комплексної системи безпеки спеціального об’єкту – це професійно спроектована, економічно вигідна та високозахищена система безпеки</td><td>1. Захист спеціальних об’єктів</td><td rowspan="3">Це сучасна та високозахищена інтегрована комплексна система безпеки з урахуванням усіх нюансів об’єкту на базі єдиної системи з єдиним програмним забезпеченням та технічною підтримкою 24/7.</td></tr>
<tr><td>2. Захист стратегічних об’єктів</td></tr>
<tr><td>3. Захист складних приватних об’єктів</td></tr>
</table>

Опис до таблиці 4.2:

W – слабка сторона;

N – нейтральна сторона;

S – сильна сторона.

Таблиця 4.2 – Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	Техніко-економічні характе-ристики ідеї	(потенційні) товари/концепції конкурентів	W	N	S
		Болід			
1	Захищеність	висока		+	
2	Технології	+		+	
3	Об’єкти	приватні	+		
4	Контакт-центр	+		+	
5	Вартість послуги	150 000 грн	+		
6	Абон.плата сервісу	25 000 грн/м		+	

4.2 Технологічний аудит ідеї проекту

Таблиця 4.3 – Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Технічна база	Болід	наявна	доступна
2	Інженерні розробки	Дисертація	наявна	доступна
3	Контакт-центр	«Контакт-центр по запросу» послуга 0-800	необхідно розробити	доступна
4	Персональний онлайн сервіс	Програмне забезпечення для ОС: Windows, Android, Mac	необхідно розробити	доступна

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Таблиця 4.4 – Попередня характеристика потенційного ринку

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	1
2	Динаміка ринку (якісна оцінка)	зростає
3	Наявність обмежень для входу (вказати характер обмежень)	відсутні
4	Сертифікація	наявна
5	Середня норма рентабельності в галузі (або по ринку), %	53%

Таблиця 4.5 – Характеристика потенційних клієнтів стартап-проекту

Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
Спеціальні об’єкти	Банківська сфера, стратегічні об’єкти, дата центри.	Залежно від цільової групи, послуга відрізнятимется через інженерні характеристики самого об’єкту. Залежно від вподобань цільових сегментів, послуга комплектується різного роду додатками для зручності користування.	- надійність - захищеність - безвідмовність - економічна вигода - технологічність - технічна підтримка

Таблиця 4.6 – Фактори загроз

№	Фактор	Зміст загрози	Можлива реакція компанії
1	Незацікавленість клієнтів	Внаслідок невдалого маркетингу клієнт може не зацікавитись послугами	Внесення додаткових сервісних послуг та зниження цін
2	Втрата монополії	Втрата рангу єдиного гаранту якості технології	Якісне та кількісне нарощування інтенсивності

Таблиця 4.7 – Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1.Монополія	Інноваційний тип послуг	Стандартизація на високому рівні
2.Локальний	Відсутність єдиного національного постачальника послуг	Окремий підхід до кожної локальної ділянки
3.Міжгалузева	Конкуренція з іншими галузями (постачальниками апаратної частини)	Необхідність співробітництва в окремих сегментах
4.Товарно-видова	Подолання розсинхронізації відбувається за схожими технологіями, що реалізовані апаратно	За необхідності, використання приладів схожого типу

Продовження таблиці 4.7 – Ступеневий аналіз конкуренції на ринку

5.Цінова	Можливість заощадити за допомогою діагностики	Гнучка політика цін на доступ
6.Марочна	Кожна діагностика має бути стандартизованою	Отримання монополії над стандартом синхронізації

Таблиця 4.8 – Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
	Технологічні постачальники	Необхідність пошуку постачальників	Залучення малопопулярних постачальників	Незалежність у прийнятті клієнтських рішень	Надання переваги більш авторитетним технологічним рішенням
Висновки:	Незначна	Можливість виходу на ринок є	Постачальники диктують цінову політику на обладнання	Клієнти диктують вимоги до якості	Обмеження існують лише у разі відмови від діагностики

Таблиця 4.9 – Обґрунтування факторів конкурентноспроможності

№	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)
1	Раціональніший ціновий показник	Можливість більш раціонально використати ресурсів
2	Надання персональних сервісних послуг 24/7	Сервісна підтримка апаратної та програмної частини
3	Синхронізованість	Синхронізація з усіма ОС.
4	Спектр застосувань	Використання для ряду потреб користувачів.

Таблиця 4.10 – Порівняльний аналіз сильних та слабких сторін стартапу

№	Фактор конкуренто-спроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні						
			-3	-2	-1	0	1	2	3
1	Раціональніший ціновий показник	13			+				
2	Надання персональних сервісних послуг 24/7	15	+						
3	Синхронізованість	20		+					
4	Спектр застосувань	17	+						

Таблиця 4.11 – SWOT – аналіз стартап-проекту

Сильні сторони:, надання персональних сервісних послуг 24/7, синхронізованість	Слабкі сторони: раціональніший ціновий показник
Можливості: використання для ряду потреб користувачів	Загрози: незацікавленість клієнтів, втрата монополії

4.4 Розроблення ринкової стратегії проекту

Таблиця 4.12 – Вибір цільових груп потенційних споживачів

№	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Банки	Висока	Високий	Середній	Середня
2	Дата центри	Висока	Високий	Середній	Середня
3	Страт. об’єкти	Середня	Високий	Висока	Низька
Які цільові групи обрано: банки та дата центри.					

Таблиця 4.13 – Визначення базової стратегії розвитку

№	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
1	Створення гаранту якості державного рівня	Встановлення єдиного універсального стандарту	Розробка нових власних рішень	Стратегія диференціації
2	Дешевизна проекту	Раціональніші витрати на обладнання, та послуги	Відомі партнер на умовах лояльності та взаємовигоди	Стратегія лідерства по витратах

Таблиця 4.14 – Визначення базової стратегії конкурентної поведінки

№	Чи є проект «пер-шопрохідцем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конку-рентної поведінки
1	так	Забирати існуючих та шукати нових	Використання технічної і програмної бази конкурента на умовах договору	Стратегія виклику лідера

Таблиця 4.15 – Визначення стратегії позиціонування

№	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкуренто-спроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сфо-рмувати комплексну позицію власного проекту (три ключових)
1	Висока якість послуг	Стратегія диференціації	Синхронізова-ність	Якість, надійність, сервісність
2	Мінімальні витрати	Стратегія лідерства по витратах	Широкий спектр застосування	Дешевизна, раціональність, тех. підтримка

4.5 Розроблення маркетингової програми стартап-проекту

Таблиця 4.16 – Визначення ключових переваг концепції потенційного товару

№	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити
1	Якість	Висока якість, сервісність	сервісність
2	Дешевизна	Раціональне використання коштів	дешевизна

Таблиця 4.17 – Опис трьох рівнів моделі товару

Рівні товару	Сутність та складові		
I. Товар за задумом	Дешевий якісний товар та послуги, стандартизована якість послуг та обладнання		
II. Товар у реальному виконанні	Властивості/характеристики:	М/Нм	Вр/Тх /Тл/Е/Ор
	1) Варстість обслуговування, 2) Кількість елементів 3) Строк безвідмовної праці 4) Технологічна собівартість товару	1) М 2) М 3) М 4) М	1)Е 2) Пр 3)Нд 4)Тх
	Якість: держстандарт якості, високоякісні технології		
III. Товар із підкрі-пленням	До продажу – діагностика, обладнання, кріплення, дод.елементи живлення Після продажу – персональний онлайн сервіс		

Таблиця 4.18 – Визначення меж встановлення ціни

№	Рівень цін на послуги замінники	Рівень цін на послуги аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на то-вар/послугу
1	100-150 тис. грн	100-150 тис. грн	Середній	100-130 тис. грн

4.6 Висновки

Комерціалізацію стартап-проекту інженерні рішення з проектування інтегрованої комплексної системи безпеки спеціального об’єкту після проведення детального аналізу, можна вважати доцільною. На дану пропозицію на ринку присутній значний попит з молоді, наразі він не задовольняється послугами замінниками. Рентабельніть на ринку послуг насамперед обумовлена широким спектром застосування та персональним сервісом, доступним клієнтам 24/7.

Впровадження є перспективним, адже основними групами клієнтів є різні цільові аудиторії. Конкурентноспроможність проекту обумовлена відсутністю аналогів з широким спектром застосування і наявністю лише товарів замінників, що, власне, і є основним бар’єром входження на ринок.

Обраною альтернативою впровадження було обрано – заключення договорів з виробником технічної бази та банківською сферою.

Імплементація проекту доцільна оскільки рентабельність та зацікавленість потенційних груп клієнтів створює досить сприятливі умови для розвитку проекту.

ВИСНОВКИ

Магістерська дисертація розкриває особливості організації інтегрованої комплексної системи безпеки спеціального об’єкту.

За результатами аналізу отримані наступні висновки:

1. В першому розділі роботи визначено основні чинники, які необхідно враховувати при проектуванні домашньої охоронної системи. Знайдено, що на основі існуючих технічних рішень розглянута система не може у повній мірі впроваджена при створенні прототипу комплексної інтегрованої системи безпеки. Зокрема, розглянута система сигналізації та елементи системи відеонагляду не можуть забезпечити підвищений рівень захисту. Це обумовлено тим, насамперед, що характеристики таких систем не відповідають нормам при проектуванні комплексної системи охорони спеціального об’єкту.

2. В другому розділі роботи проведено аналіз технічних засобів, які утворюють структуру сучасної комплексної системи охорони. Знайдено, що розглянуті елементи відрізняються у схемотехнічому виконанні тим, що різні функції системи можна реалізувати на основі одного обладнання. Зокрема, це стосується системи сигналізації та системи пожежної безпеки, де сигнали тривоги можуть бути одночасно використані як мітки до спрацювання системи пожежної безпеки. Додатково в цій частині роботі проведено вибір основніх складових системи відео нагляду та визначено її структуру і на її основі знайдені технічні особливості, як варто враховувати при проектуванні аналогічних систем охорони об’єктів.

3. На основі спецалізованого програмного забезпечення СКС-Експерт та IP Video System Design Tool визначено основні етапи створення проекту інтегрованої системи охорони приміщення спеціального призначення і наведено рекомендації щодо налаштування та з’єднання елементів цієї комплексної інтегрованої системи безпеки на основі новітніх програмних і інженерних рішень. З’ясовано, що інструменти в розглянутих програмах

дозволяють, наприклад, що стосується системи відеонагляду, провести визначення місць розташування мережних відеокамер, які дозволять усунутив процесі створення реального проекту “сліпі” зони в тих місцях приміщення, де найвищий рівень захисту повинен бути забезпечений згідно вимог замовника на 100 відсотків.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Волхонський В.В. Системи охоронної сигналізації: 2-е вид. СПб.: Екополіс і культура, 2005. 204 с.

2. Волковіцький В.Д., Волхонський В.В. цифрові системи ТВ-спостереження. Безпека, достовірність, інформація. СПб.: 2009 38-47 с.

3. Ворона В.А., Тихонов В.А. Системи контролю і управління доступом. М.: Гаряча лінія - Телеком, 2010. 272 с

4. Гедзберг Ю.М. Охоронне телебачення. М.: Гаряча лінія - Телеком, 2005. 312 с.

5. Двинских В.І. Аналіз вразливості системи охорони. оцінки показників уразливості. Офіційний сайт охоронно-інформаційного агентства Каскад-Сервіс. Харків: 2009. 78 с.

6. Крахмальов А.К. Перспективи розвитку інтегрованих системи безпеки. платформи інтеграції. Системи безпеки. СПб. 2010. 146-148 с.

7. Круглов Герман, Професійне відеоспостереження. Практика і технології аналогового і цифрового відеоспостереження, 2-е вид.: Пер. з англ. М.: Сек'юріті Фокус (Security Focus), 2010. 640 с.

8. Лукьяніца А.А., Шишкін А.Г. Цифрова обробка відеозображень.М.: «Ай-Ес-Ес Прес», 2009. 267 с.

9. Магауенов Р.Г. Системи охоронної сигналізації: основи теорії і принципи побудови. Навчальний посібник для вузів. 2-вид. М.: Гаряча лінія – Телеком. 2008. 496 с.

10. Омельянчук А.М. Формування системи комплексної безпеки. Частина 2. Підготовка техзавдання і проектування. Системи безпеки. СПб. 2009. 114-117 с.

11. Румянцев М.Н. Ефективна Систма контролю та управління доступом на великому НПЗ. досвід заводу «Славнефть-Янос» (Ярославль). Системи безпеки. СПб. 2011. 128-130 с.

12. Синилов В. Г. Системи охоронної, пожежної та охоронно-пожежної сигналізації. Підручник для поч. проф. освіти. 5-е вид. М.: Видавничий центр «Академія» 2010. 512 с.

ДОДАТОК А
ABSTRACT

Nowadays, ensuring one's own security as well as the protection of movable and immovable property has become not a whim but a necessity. The solution to this problem is possible only with the competent equipping of security systems with modern highly reliable technical means of protection. More and more people are becoming clients of security companies, including owners of apartments, private estates, businesses, organizations, vehicles, and even strategic state-owned entities.

Demand for the latest and most reliable security systems is on the rise, which is why manufacturers of such systems are constantly in an atmosphere of fierce competition that drives them to rapid technical development. That is why I consider the development of an advanced model of integrated integrated security system for a special object a topical topic of a master's thesis.

The purpose of the research is to develop recommendations for the creation, use, implementation and improvement of technologies of integrated integrated security systems at a special facility. Thus, it is supposed to create a well-equipped model of a special object with modern highly reliable technical means of security systems.

The master's dissertation reveals the peculiarities of organizing an integrated complex security system for a special object.

1. An analytical review of the home security systems of the premises is given, the classification, the structure, the topology of such systems are introduced, and the shortcomings in comparison with the integrated complex security systems are revealed.

2. The basic principles for implementation of a highly protected integrated complex security system of a special object are formulated. In terms of integration, these are:

– The highest (global) layer involves the integration of integrated security systems with other information systems, is a computer network type "client/server" on the basis of Ethernet, with the TCP/IP exchange protocol and the use of professional operating systems (OS) type Windows or Linux. This layer provides

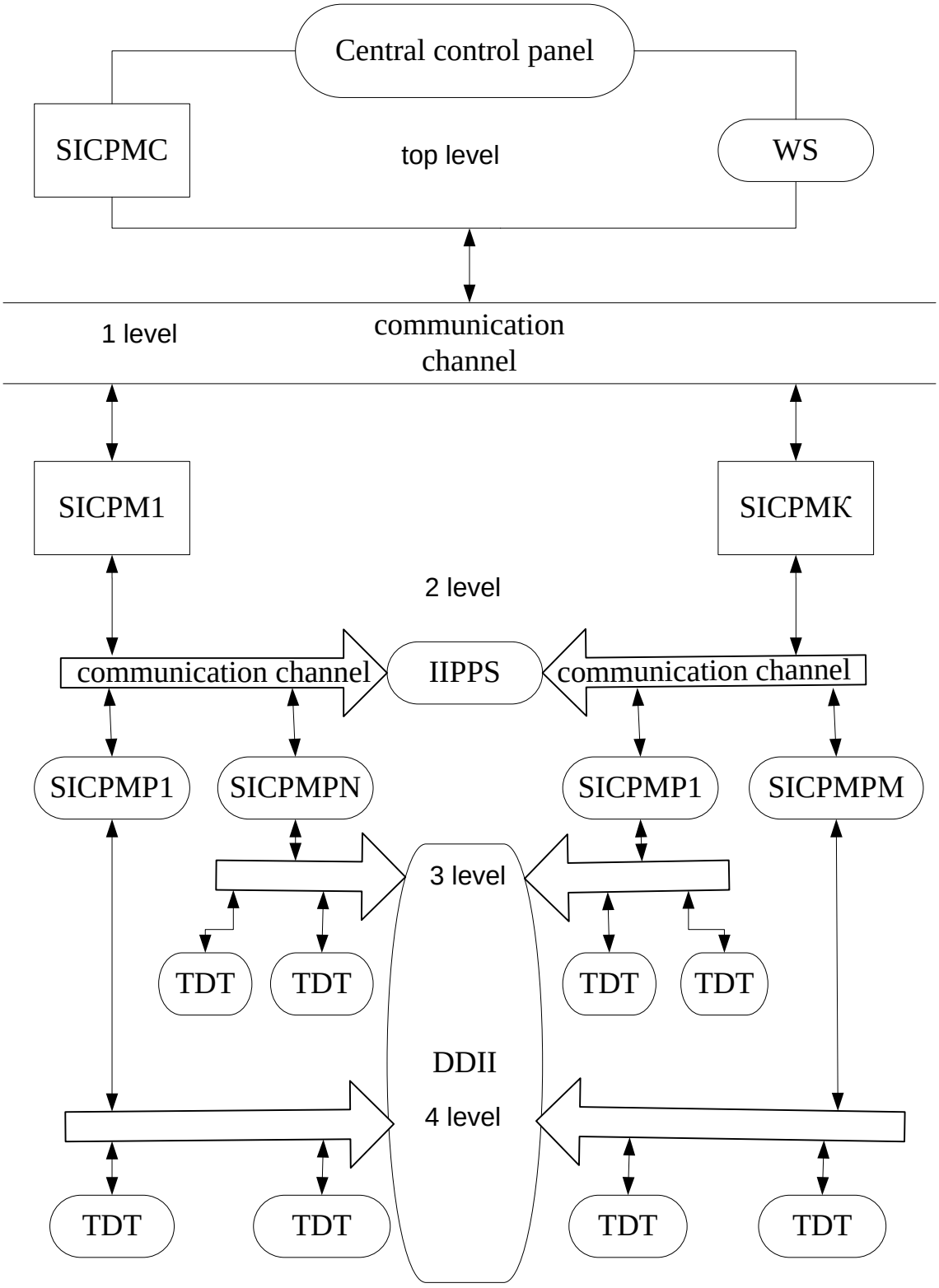
communication between the server and the workstations of the operators, and provides management of the integrated security system using the software. This level requires high reliability and protection against unauthorized access.

– The first (system) level involves the information interaction of the system of information collection and processing and management of individual security subsystems and counteraction and threat elimination subsystems within the integrated security system (these may be control and monitoring devices that provide control of security and fire protection systems, and controllers). At this level, the the system of information collection and processing and management is central or central processor (server) integrates all subsystems.

– The second (system) layer involves the integration of local (or peripheral) systems for collecting and processing information of individual security subsystems. Integration can be accomplished through software over communication channels or through peripheral processing systems integration interfaces. In this case, a combination of vertical integration (communication between controllers and computers of subsystems) and horizontal integration (communication between homogeneous controllers in each of the subsystems) at the vertical level is most commonly used interface RS-232, at the horizontal level RS-485 designed to build industrial-grade networks with good noise immunity and sufficient data rate.

– The third (modular) level involves the interaction between the the system of information collection and processing and management peripheral and the threat detection tools of its subsystems. Local value controllers control a small group of sensors, camcorders, readers, actuators, etc. As a rule, RS-485, RS-232 or standard Wigand 26 interfaces are used at this level. Alerts, fire extinguishers and fire extinguishers, address control units with relay and potential outputs are also located at this level [12].

– The fourth (lower) layer involves the interaction of the threat detection tools of the various security subsystems through generalized loops or appropriate interfaces for the integration of detection devices.



Picture – The levels of integration of the various elements of an integrated integrated security system

3. The project of the integrated integrated security system of a special facility on the basis of the technical means of protection of the "Bolid" was researched and developed, as they have the following advantages:

– combined security and fire sensors with built-in alarm and sound alarm;

– continuous survey of sensors every 38 seconds;

– high security communication channel, information is transmitted in a separate cable network via the RS-485 and RS-232 interface;

– high noise immunity;

– number of sensors connected to one controller 120;

– convenient interface for the central control panel, regular updates and round-the-clock support;

– communication at the physical level is provided by a two-wire line fireproof;

– interoperability with other systems of this manufacturer, which facilitates the installation and management of an integrated security system;

– Receives and records video in MJPEG, MPEG-4, H.264 formats directly into AVI containers. It is also possible to receive and record audio in PCM, G.711, G.726, AAC codecs;

– The production of the “Bolid” production software not only allows to monitor, but also to identify people and events.

Disadvantages:

– Monopoly of one manufacturer of technical means of protection and software, which can lead to negligence of information or diversion. In order to avoid such situations, projects should be created, commissioned and maintained by another trusted firm or engineers.

According to the results of the analysis the following conclusions were obtained:

1. The first section identifies the main factors to consider when designing a home security system. It was found that, based on existing technical solutions, the considered system could not be fully implemented when creating a prototype of a

comprehensive integrated security system. In particular, the alarm system under consideration and the elements of the video surveillance system cannot provide an increased level of protection. This is primarily due to the fact that the characteristics of such systems do not meet the standards when designing a comprehensive security system for a special object.

2. The second section of the paper analyzes the technical means that make up the structure of a modern complex security system. It is found that the elements considered differ in circuit design in that the various functions of the system can be implemented on the basis of the same equipment. This applies in particular to the alarm system and the fire safety system, where alarms can be used simultaneously as tags for the fire safety system to be triggered. Additionally, in this part of the paper, a selection of the main components of a video surveillance system is made and its structure is determined and technical characteristics are found on the basis of this, as it should be taken into account when designing similar systems of object security.

3. On the basis of the specialized software SCS-Expert and IP Video System Design Tool Tool the main stages of creation of the project of the integrated security system of the special purpose premises are defined and the recommendations on setting up and connection of elements of this integrated integrated security system are based on the latest software and engineering solutions. It has been found that the tools in the programs in question allow, for example, for the CCTV system, to determine the locations of network camcorders, which will eliminate the process of creating a real blind project area in those areas where the highest level of protection should be provided as required customer 100 percent.